# 200A Homework 5

James Harbour

October 28, 2025

## Problem 1

Suppose $n$ is a positive integer. Prove that every group of order $n$ is cyclic if and only if $\gcd(n, \phi(n)) = 1$.
*Hint.* One of the fundamental results in finite group theory is the following result of Burnside.

**Theorem 0.0.1** (Burnside's Normal $p$-Complement)**.** *Suppose $G$ is a finite group, $P$ is a Sylow $p$-subgroup, and $P \subseteq Z(N_G(P))$. Then there exists a normal subgroup $N$ of $G$ such that $|N| = |G/P|$.*

You may use this theorem without proof. Use strong induction on $n$ to show that every group of order $n$ is cyclic if $\gcd(n, \phi(n)) = 1$. Observe that $\gcd(n, \phi(n)) = 1$ implies that $n$ is square-free. Notice that if $m \mid n$, then $\gcd(m, \phi(m)) = 1$. By the strong induction hypothesis, deduce that every proper subgroup of $G$ is cyclic. Deduce that if a Sylow $p$-subgroup is not normal, then $N_G(P)$ is cyclic. Use Burnside's normal complement.

*Proof.* We induct strongly on $n \in \mathbb{N}$ in the statement that $\gcd(n, \phi(n)) = 1$ implies every group of order $n$ is cyclic. $\square$

## Problem 2

In this problem, you prove that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ if $n \geq 7$.

**(a)**: Suppose $\phi$ is an automorphism of $S_n$ which sends transpositions to transpositions; that means $\phi((a\,b))$ is a 2-cycle for every $1 \leq a < b \leq n$. Prove that $\phi$ is an inner automorphism. (For this part it is enough to assume that $n \geq 5$.)

*Proof.* Let $K_n$ denote the complete, undirected graph on $n$ vertices and label the vertices $1, 2, \dots, n$. Let $T_1 \subseteq S_n$ denote the set of transpositions in $S_n$. Note that we have a bijection $T_1 \to E(K_n)$ given by $\tau = (i\,j) \mapsto \mathrm{supp}(\tau) = \{i, j\}$, so we identify the two sets.

As $\varphi$ is an automorphism, $|\varphi(T_1)| = |T_1|$, whence the assumption that $\varphi(T_1) \subseteq T_1$ implies $\varphi(T_1) = T_1$. Hence, under the identification of $T_1$ with $E(K_n)$, the function $\varphi|_{T_1}$ furnishes a bijection $\varphi|_{T_1} : E(K_n) \to E(K_n)$. We will show that this bijection is induced from a graph isomorphism of $K_n$.

Fix $i \in \{1, \dots, n\}$ and suppose that $\tau, \tau' \in T_1$ with $\tau \neq \tau'$ and $i \in \mathrm{supp}(\tau) \cap \mathrm{supp}(\tau')$. Then there are $j, k \in \{1, \dots, n\} \setminus \{\}$ with $j \neq k$such that $\tau = (i\,j)$ and $\tau' = (i\,k)$.

$$3 = o(\varphi((i\,k\,j))) = o(\varphi(\tau\tau')) = o(\varphi(\tau)\varphi(\tau'))$$

Note that $\varphi(\tau)$ and $\varphi(\tau')$ are transpositions. If $\operatorname{supp}(\varphi(\tau)) \cap \operatorname{supp}(\varphi(\tau')) = \emptyset$, then $o(\varphi(\tau)\varphi(\tau')) = 4$ which contradicts the above equation. Thus $\operatorname{supp}(\varphi(\tau)) \cap \operatorname{supp}(\varphi(\tau')) \neq \emptyset$. If $|\operatorname{supp}(\varphi(\tau)) \cap \operatorname{supp}(\varphi(\tau'))| = 2$ , then $\varphi(\tau) = \varphi(\tau')$ contradicting that $\varphi$ is injective. Thus $|\operatorname{supp}(\varphi(\tau)) \cap \operatorname{supp}(\varphi(\tau'))| = 1$.

Put simply, the above explanation shows that for any two distinct transpositions $\tau, \tau'$ which share an element, it follows that $\varphi(\tau)$ and $\varphi(\tau')$ also share exactly one element. Rephrasing this inside of $E(K_n)$, for any two distinct edges $e, e'$ which share a vertex, it follows that $\varphi(e)$ and $\varphi(e')$ also share exactly one vertex.

Let $\mathcal{F} := \{e \in E(K_n) : i \text{ is incident with e}\} = \{(i\, j) \in S_n : j \in \{1, \ldots, n\} \setminus \{i\}\}$. Then for any distinct $\tau, \tau' \in \mathcal{F}$, $|\operatorname{supp}(\varphi(\tau)) \cap \operatorname{supp}(\varphi(\tau'))| = 1$. Fix distinct $e, e' \in \mathcal{F}$ and write $e = (i\, \alpha)$, $e' = (i\, \beta)$ with $i \neq \alpha \neq \beta$. As

$$|\operatorname{supp}(\varphi((i\, \alpha))) \cap \operatorname{supp}(\varphi((i\, \beta)))| = 1,$$

there are $a \neq b_1 \neq b_2$ in $\{1, \ldots, n\}$ such that $\varphi((i\, \alpha)) = (a\, b_1)$ and $\varphi((i\, \beta)) = (a\, b_2)$. Suppose $f \in \mathcal{F}$ is any other edge/transposition with $f \neq e, e'$. Write $f = (i\, \gamma)$ where $\gamma \neq \alpha, \beta, i$. Suppose, for the sake of contradiction, that $a \notin \operatorname{supp}(\varphi((1\, \gamma)))$. As

$$|\operatorname{supp}(\varphi((i\, \gamma))) \cap \operatorname{supp}(\varphi((i\, \beta)))| = 1,$$
$$|\operatorname{supp}(\varphi((i\, \gamma))) \cap \operatorname{supp}(\varphi((i\, \alpha)))| = 1,$$

it follows that $\varphi((i\, \gamma)) = (b_1\, b_2)$. Then we may write

$$\varphi((\alpha\, \beta)) = \varphi((i\, \alpha)(i\, \beta)(i\, \alpha)) = (a\, b_1)(a\, b_2)(a\, b_1) = (b_1\, b_2) = \varphi((i\, \gamma))$$

which contradicts the injectivity of $\varphi$. Thus we have shown

$$\left| \bigcap_{e \in \mathcal{F}} \varphi(e) \right| = 1,$$

whence we may define a map $\Phi : K_n \to K_n$ by

$$\Phi(i) := \widehat{i} \quad \text{where } \widehat{i} \in \bigcap_{\substack{e \in E(K_n) \\ i \in e}} \varphi(e).$$

We claim that $\Phi$ is a graph automorphism. We show injectivity first. Suppose $1 \neq i \in \{1, \ldots, n\}$. We will show that $\Phi(1) \neq \Phi(i)$, whence injectivity follows without loss of generality.
Let $k = \Phi(1)$ and suppose, for the sake of contradiction, that $k = \Phi(i)$. Choose $j \in \{1, \ldots, n\}$ such that $j \neq 1, i$. Then using the same logic with supports as above, we may write

$$\varphi((i\, 1)) = (k\, a)$$
$$\varphi((i\, j)) = (k\, b)$$
$$\varphi((1\, j)) = (k\, c)$$

with $a \neq b \neq c$. Then observe that

$$(k\, b) = \varphi((i\, j)) = \varphi((i\, 1)(1\, j)(i\, 1)) = (k\, a)(k\, c)(k\, a) = (a\, c),$$

whence $a \neq b$ implies that $a = k$, contradicting that $\varphi$ sends transpositions to transpositions. Thus $\Phi$ is injective, whence size considerations give that $\Phi$ is bijective.

Fix $i \neq j \in \{1, \dots, n\}$. Then as $i, j \in (i\, j)$, it follows that

$$\Phi(i) = \bigcap_{\substack{e \in E(K_n) \\ i \in e}} \varphi(e) \in \varphi((i\, j)) \quad \text{and} \quad \Phi(j) = \bigcap_{\substack{e \in E(K_n) \\ i \in e}} \varphi(e) \in \varphi((i\, j)).$$

Using the injectivity of $\Phi$, we see that

$$\varphi((i\, j)) = (\Phi(i), \Phi(j)) \in E(K_n).$$

As $\varphi$ is a bijection on $E(K_n)$, it follows that $\Phi$ is an automorphism of $K_n$ whence it induces a permutation $\Phi \in S_n$ by considering only the map on vertices. But then, inside $S_n$,

$$\varphi((i\, j)) = (\Phi(i)\, \Phi(j)) = \Phi(i\, j)\Phi^{-1}$$

for all $i \neq j$, whence $\varphi$ is inner as transpositions generate $S_n$. □

**(b)**: Suppose $\phi$ is an automorphism. Prove that for all $\sigma_1, \sigma_2 \in S_n$, $\phi(\sigma_1)$ and $\phi(\sigma_2)$ are conjugate if and only if $\sigma_1$ and $\sigma_2$ are conjugate. (This is true for an automorphism of any group.)

*Proof.* Let $G$ be any group and $\varphi \in \mathrm{Aut}(G)$. Suppose that $g_1, g_2 \in G$ are conjugate, so there is some $x \in G$ such that $g_1 = x g_2 x^{-1}$. Then

$$\varphi(g_1) = \varphi(x g_2 x^{-1}) = \varphi(x)\varphi(g_2)\varphi(x)^{-1},$$

whence $\varphi(g_1)$ and $\varphi(g_2)$ are conjugate.

On the other hand, suppose that $g_1, g_2 \in G$ are such that $\varphi(g_1)$ and $\varphi(g_2)$ are conjugate. Then there is some $y \in G$ such that $\varphi(g_1) = y\varphi(g_2)y^{-1}$. As $\varphi$ is an automorphism, there is some $x \in G$ such that $y = \varphi(x)$. Then

$$\varphi(g_1) = y\varphi(g_2)y^{-1} = \varphi(x)\varphi(g_2)\varphi(x)^{-1} = \varphi(x g_2 x^{-1}),$$

whence as $\varphi$ is an automorphism it follows that $g_1 = x g_2 x^{-1}$, so $g_1$ and $g_2$ are conjugate. □

**(c)**: Let $T_k$ be the set of permutations with cycle type

$$(2, \dots, 2 \ k \text{ times}, \ 1, \dots, 1 \ n - 2k \text{ times}).$$

For instance, $T_1$ is the set of 2-cycles. Prove that

$$|T_k| = \frac{n(n-1)\cdots(n-2k+1)}{k! 2^k} \geq \frac{n(n-1)}{2} \cdot \frac{(2k-2)!}{k! 2^{k-1}},$$

for a positive integer $k \leq n/2$.

*Proof.* First choosing the $n - 2k$ 1-cycles gives $\binom{n}{n-2k}$ choices. Then out of the remaining $2k$ elements, we iteratively choose pairs for each cycle, which after correcting for the fact that we do not care about the ordering of the $k$ pairs we have chosen, gives $\frac{1}{k!}\binom{2k}{2}\binom{2k-2}{2}\cdots\binom{2k-(2k-2)}{2}$ choices. Hence, in total

$$\begin{aligned} |T_k| &= \binom{n}{2k} \cdot \frac{1}{k!}\binom{2k}{2}\binom{2k-2}{2}\cdots\binom{2k-(2k-2)}{2} \\ &= \frac{n(n-1)\cdots(n-2k+1)}{k!(2k)!} \cdot \frac{2k(2k-1)}{2} \cdot \frac{(2k-2)(2k-3)}{2} \cdots \frac{3 \cdot 2}{2} \\ &= \frac{n(n-1)\cdots(n-2k+1)}{k! 2^k}. \end{aligned}$$

Now, using that $k \leq n/2$ or equivalently $n \geq 2k$, we estimate

$$\begin{aligned}\frac{n(n-1)\cdots(n-2k+1)}{k!2^k} &= \frac{n(n-1)}{2}\cdot\frac{(n-2)(n-3)\cdots(n-2k+1)}{k!2^{k-1}} \\ &\geq \frac{n(n-1)}{2}\cdot\frac{(2k-2)(2k-3)\cdots(2k-2k+1)}{k!2^{k-1}} = \frac{n(n-1)}{2}\cdot\frac{(2k-2)!}{k!2^{k-1}}.\end{aligned}$$

□

**(d)**: Prove that for every $\phi \in \mathrm{Aut}(S_n)$, there exists an integer $k$ such that $\phi(T_1) = T_k$.

*Proof.* Fix $\varphi \in \mathrm{Aut}(S_n)$ Let $\sigma \in T_1$ and suppose that $\varphi(\sigma)$ has cycle type $l_1 \leq l_2 \leq \cdots \leq l_m$. Then, as $\varphi$ is an automorphism,

$$2 = o(\sigma) = o(\varphi(\sigma)) = \mathrm{lcm}(l_1, l_2, \ldots, l_m),$$

whence each $l_i \in \{1, 2\}$ and at least one $l_i$ is equal to 2. Thus, $\varphi(\sigma) \in T_k$ for some $k \in \mathbb{N}$. As every element in $T_1$ is conjugate, it follows by part (b) that every element in $\varphi(T_1)$ is conjugate. Thus, every element in $\varphi(T_1)$ has the same cycle type, namely that of $\sigma$, so $\varphi(T_1) \subseteq T_k$.

Now fix $\sigma \notin T_1$. Suppose, for the sake of contradiction, that $\varphi(\sigma) \in T_k$. Fix $\tau \in T_1$. As $T_k$ is a conjugacy class, $\varphi(\sigma)$ is conjugate to $\varphi(\tau)$, whence $\sigma$ is conjugate to $\tau$. As $T_1$ is a conjugacy class, it follows that $\sigma \in T_1$, which is a contradiction. Thus $\sigma \notin T_k$.

□

**(e)**: Prove that for every $\phi \in \mathrm{Aut}(S_n)$, $\phi(T_1) = T_1$. Deduce that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$.

*Proof.* Fix $\varphi \in \mathrm{Aut}(S_n)$. Then there is some $k \in \mathbb{N}$ such that $\varphi(T_1) = T_k$. Then, we compute

$$\begin{aligned}|T_1| = |\varphi(T_1)| = |T_k| &\geq \frac{n(n-1)}{2}\cdot\frac{(2k-2)!}{k!2^{k-1}} \\ &= |T_1| \cdot \frac{(2k-2)!}{k!2^{k-1}}\end{aligned}$$

whence it must hold that

$$1 \geq \frac{(2k-2)!}{k!2^{k-1}}.$$

Suppose, for the sake of contradiction, that $k > 1$. Then

$$\begin{aligned}1 \geq \frac{(2k-2)!}{k!2^{k-1}} &= \frac{2(k-1)(2k-3)2(k-2)(2k-5)\cdots 2(2)\cdot 3\cdot 2(1)\cdot 1}{k!2^{k-1}} \\ &= \frac{2^{k-1}(k-1)!(2k-3)(2k-5)\cdots 5\cdot 3\cdot 1}{2^{k-1}k!} \\ &= \frac{(2k-3)(2k-5)\cdots 5\cdot 3\cdot 1}{k} \\ &= \left(2 - \frac{3}{k}\right)(2k-5)\cdots 5\cdot 3 \\ &\geq \left(2 - \frac{6}{n}\right)(2k-5)\cdots 5\cdot 3\end{aligned}$$

which is absurd as $n \geq 7$ implies that $\left(2 - \frac{6}{n}\right) > 1$.

Thus we have shown $\varphi(T_1) = T_1$. Hence, by part (a), $\varphi \in Inn(S_n)$. □

*Hint.* Consider the complete graph with $n$ vertices. Notice that there is a bijection between 2-cycles and edges of this graph. If an automorphism $\phi$ sends 2-cycles to 2-cycles, then it induces a bijection on the edges of this graph. Observe that two 2-cycles $\tau_1$ and $\tau_2$ do not commute if and only if the corresponding edges of $\tau_1$ and $\tau_2$ have a vertex in common. Use this property to show that the induced map on edges gives an automorphism of the graph, and hence a permutation $\sigma$ on the set of vertices. Prove that $\phi$ is conjugation by $\sigma$.

# Problem 3

For every group $G$, the group of outer automorphisms is

$$\mathrm{Out}(G) := \frac{\mathrm{Aut}(G)}{\mathrm{Inn}(G)}.$$

Let $\mathrm{Cl}(G)$ be the set of conjugacy classes of $G$.
**(a)**: Prove that

$$(\theta\,\mathrm{Inn}(G)) \cdot [a] := [\theta(a)]$$

is a well-defined action of $\mathrm{Out}(G)$ on $\mathrm{Cl}(G)$, where $[g]$ denotes the conjugacy class of $g$ in $G$.

**(b)**: Argue why

$$f : \mathrm{Cl}(G) \to \mathbb{Z} \times \mathbb{Z}, \quad f([g]) := (o(g), |[g]|)$$

is fixed along an $\mathrm{Out}(G)$-orbit.

**(c)**: Prove that $\mathrm{Aut}(S_n) \cong \mathrm{Inn}(S_n)$ if $n \neq 6$.

**(d)**: Prove that $\mathrm{Aut}(S_n) \cong S_n$ if $n \neq 2, 6$.
*Hint.* Use an argument similar to part (a) of Problem 2.

# Problem 4

Suppose $n$ is an integer at least 2.
**(a)**: Prove that $S_n = \langle (1\,2), (1\,2\,\cdots\,n) \rangle$. (This means the smallest subgroup of $S_n$ containing $(1\,2)$ and $(1\,2\,\cdots\,n)$ is $S_n$.)

**(b)**: Suppose $p$ is prime, $\tau \in S_p$ is a 2-cycle, and $\sigma \in S_p$ is an element of order $p$. Prove that $S_p = \langle \tau, \sigma \rangle$.
*Hint.* Let $\gamma := (1\,2)(1\,2\,\cdots\,n) = (2\,3\,\cdots\,n)$. Consider $\gamma^i(1\,2)\gamma^{-i}$ and use this to show that all 2-cycles are in the group generated by these elements.
For the second part, think of permutations of $\mathbb{Z}/p\mathbb{Z} = \{0, \ldots, p-1\}$. Notice that an element of order $p$ is a $p$-cycle. After relabelling, assume that

$$\sigma : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \quad \sigma(x) := x + 1.$$

After another relabelling, assume $\tau = (0\,a)$ for some $a \neq 0$. Consider $\sigma^i \tau \sigma^{-i} = (i\,a+i)$. Use this to obtain that $(ka, (k+1)a)$ is in the group for every $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. Inductively show that $(0, ka)$ is in this group for every $k \in (\mathbb{Z}/p\mathbb{Z})^\times$. Deduce that $(0\,1)$ is in this group. Use the first part.

# Problem 5

**(15-puzzle)** In a 15-puzzle, a player can rearrange the numbers 1–15 by sliding the numbers into the empty spot.
Starting with the position

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | |

can we get to the following position?

| | | | |
|---|---|---|---|
| 2 | 1 | 3 | 4 |
| 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | |

*Hint.* Think about each position in the 15-puzzle as a permutation in $S_{16}$. Every sliding move is a 2-cycle. Argue why we need an even number of sliding moves to go from the initial position to the second given position.

# Problem 6

Suppose $G$ is a finite group of order $2^k m$ where $k$ is a positive integer and $m$ is odd. Suppose $G$ has a cyclic Sylow 2-subgroup. Prove that $G$ has a characteristic subgroup of order $m$.
*You are not allowed to use Burnside's p-complement theorem for this problem.*
*Hint.* Suppose $\phi : G \to S_G$ is the embedding given by the action of $G$ on itself by left translations. Prove that $\varepsilon \circ \phi : G \to \{\pm 1\}$ is not trivial. Show that $\ker(\varepsilon \circ \phi)$ is a characteristic subgroup of index 2. By induction, prove that for every integer $1 \leq i \leq k$, $G$ has a characteristic subgroup of index $2^i$.