Zack Garza

1) Let $\sigma = (i_1 \; i_2 \cdots i_m) \in S_n$ be a cycle, where $m \leq n$, so we have $\boxed{i_j \xmapsto{\sigma} i_{j+1 \bmod m}}$ for each $1 \leq j \leq m$.

Now let $\tau = (t_1 \; t_2 \cdots t_k) \in S_n$ be another cycle.

Note that wlog we can assume τ is a single cycle; if $\tau = \alpha\beta$ is the product of 2 disjoint cycles $\alpha, \beta \in S_n$, then $\tau^{-1} = \beta^{-1}\alpha^{-1}$ and so

$$\tau^{-1}\sigma\tau = \beta^{-1}\underbrace{\alpha^{-1}\sigma\alpha}\beta := \beta^{-1}\sigma'\beta,$$

where σ' will inductively be a single cycle, since if $\sigma' = (s_1 \; s_2 \cdots s_m)$ then $\alpha^{-1}\sigma'\alpha = (\alpha(s_1) \; \alpha(s_2) \cdots \alpha(s_m))$.

We want to show that

$$\tau\sigma\tau^{-1} = (\tau(i_1) \; \tau(i_2) \cdots \tau(i_m)), \quad \text{i.e.}$$

$$\tau(i_j) \xmapsto{\tau\sigma\tau^{-1}} \tau(i_{j+1 \bmod m})$$

So consider what happens to a fixed $\tau(i_j)$:

- Applying τ^{-1}: $\tau(i_j) \xmapsto{\tau^{-1}} i_j$ (since $\tau^{-1}\tau = id$)
- Applying σ: $i_j \xmapsto{\sigma} i_{j+1 \bmod m}$ (by $\star$)
- Applying τ: $i_{j+1 \bmod m} \xmapsto{\tau} \tau(i_{j+1 \bmod m})$ (by defn.)

So $\tau(i_j) \xmapsto{\tau} i_j \xmapsto{\sigma} i_{j+1 \bmod m} \xmapsto{\tau} \tau(i_{j+1 \bmod m})$

$$\Rightarrow \tau(i_j) \xmapsto{\tau\sigma\tau^{-1}} \tau(i_{j+1 \bmod m}) \quad \text{as desired.} \ \blacksquare$$

---

2) <u>Claim 1</u>:

Let $\tau_{ij} = (i \ j) \in S_n$, so for $1 \leq i, j \leq n$ we have

$i \xmapsto{\tau_{ij}} j$ and $\tau_{ij}^2 = id$, and let $A = \{\tau_{ij} \mid 1 \leq i, j \leq n\}$.

Then $S_n = \langle A \rangle$.

<u>Claim 2</u>: Let

$$\sigma = (1 \ 2)$$
$$\tau = (1 \ 2 \ 3 \cdots n)$$

Then $\langle A \rangle \subseteq \langle \sigma, \tau \rangle$.

Note that if these are true, then

$$\underbrace{S_n = \langle A\rangle}_{\text{Claim 1}} \subseteq \langle \sigma, \tau \rangle \subseteq S_n \implies \underbrace{\langle \sigma, \tau\rangle = S_n}_{\text{What we want to show}}$$

Claim 2 ($\langle A\rangle \subseteq \langle \sigma,\tau\rangle$)

Since $\sigma, \tau \in S_n$ which is closed under products ($\langle \sigma,\tau\rangle \subseteq S_n$)

Proof of claim 1: Note that $\langle A\rangle \subseteq S_n$ since S_n is closed under products, so it suffices to show $S_n \subseteq \langle A\rangle$.

Let $\sigma \in S_n$. Since any element of S_n is a product of disjoint cycles, wlog we can assume σ is a single cycle. So write $\sigma = (s_1\ s_2 \cdots s_m)$ where $1 \le m \le n$; we want to show $\sigma = \prod \tau_{ij}$ for some collection of τ_{ij}'s. To this end, we have

$$\underbrace{(s_1\ s_2)}_{\tau_{s_1 s_2}}\underbrace{(s_1\ s_3)}_{\tau_{s_1 s_3}} \cdots \underbrace{(s_1\ s_m)}_{\tau_{s_1 s_m}} = \underbrace{(s_1\ s_2 \cdots s_m)}_{\sigma}$$

where we just note that $s_1 = i$ for some i and each s_k for $2 \le k \le m$ is some j. So each $(s_1\ s_k)$ is some $(i\ j)$, which is τ_{ij}. So every cycle is a product of some collection of τ_{ij}'s as desired.

Proof of claim 2:

wlog, $1 \leq i < j < n$

Let $\tau_{ij} = (i \; j) \in \langle A \rangle$; we want to write this in terms of σ and τ. By part (I), we have

$$\tau \sigma \tau^{-1} = \tau (1 \; 2) \tau^{-1} = (\tau(1) \; \tau(2))$$
$$= (2, 3) \in \langle \sigma, \tau \rangle,$$

and thus inductively,

$$\gamma^{k+1} := \tau^{k} \sigma \tau^{-k} = (k+1 \bmod n, \; k+2 \bmod n) \in \langle \sigma, \tau \rangle$$

In particular,

$$\gamma^{i} = \tau^{i-1} \sigma \tau^{-(i-1)} = (i, i+1) \in \langle \sigma, \tau \rangle$$

and so

$$\underbrace{\gamma^{i} \gamma^{i+1} \gamma^{i+2} \cdots \gamma^{j-1}}_{\in \langle \sigma, \tau \rangle} = (i, i+1)(i+1, i+2) \cdots (j-1, j) = \underbrace{(i, j)}_{\in \langle \sigma, \tau \rangle}. \quad \blacksquare$$

3) Since G is finite and abelian, we know G factors as

$$G \cong \prod \mathbb{Z}_{p_i^{\alpha_i}},$$ where the p_i are not necessarily distinct and each $\alpha_i \geq 1$.

If every p_i is distinct, then we would have $i \neq j \Rightarrow \gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$,

and so $\prod_k \mathbb{Z}_{p_k^{\alpha_k}} \cong \mathbb{Z}_{\prod_k p_k^{\alpha_k}} \cong \mathbb{Z}_{\#G}$, which would be cyclic.

So for some i, j we must have $p_i = p_j$, and so

$$G \cong \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \prod_{k \neq i,j} \mathbb{Z}_{p_k^{\alpha_k}}$$

and so $H := \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \leq G$ is a subgroup.

But then, by Cauchy's theorem $\mathbb{Z}_{p^{\alpha_1}}$ contains a subgroup

of order p, say $H_1 \leq \mathbb{Z}_{p^{\alpha_1}}$, and similarly there is an

$H_2 \leq \mathbb{Z}_{p^{\alpha_2}}$. But groups of prime order are cyclic, and so

$H_1 \cong \mathbb{Z}_p \cong H_2$.

Since $H_1 \times H_2 \leq H := \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \leq \prod \mathbb{Z}_{p_k^{\alpha_k}} \cong G$,

we have $H_1 \times H_2 \leq G$ where $H_1 \times H_2 \cong \mathbb{Z}_p \times \mathbb{Z}_p$ as desired. $\blacksquare$

4) Order $64 = 2^6$, and $p(6) = 11$, so

$$
\begin{aligned}
&6 &&\longrightarrow \mathbb{Z}_{64} \\
&5+1 &&\longrightarrow \mathbb{Z}_{32} \times \mathbb{Z}_2 \\
&4+2 &&\longrightarrow \mathbb{Z}_{16} \times \mathbb{Z}_4 \\
&3+3 &&\longrightarrow \mathbb{Z}_8 \times \mathbb{Z}_8 \\
&4+1+1 &&\longrightarrow \mathbb{Z}_{16} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
&3+2+1 &&\longrightarrow \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \\
&2+2+2 &&\longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \\
&3+1+1+1 &&\longrightarrow \mathbb{Z}_8 \times (\mathbb{Z}_2)^3 \\
&2+2+1+1 &&\longrightarrow (\mathbb{Z}_4)^2 \times (\mathbb{Z}_2)^2 \\
&2+1+1+1+1 &&\longrightarrow \mathbb{Z}_4 \times (\mathbb{Z}_2)^4 \\
&1+1+1+1+1+1 &&\longrightarrow (\mathbb{Z}_2)^6
\end{aligned}
$$

Order $96 = 2^5 \cdot 3^1$, and $p(5)p(1) = 7 \cdot 1 = 7$

(Partition of 5, Partition of 3)	Distinct abelian group
$(5, 1)$ $\longrightarrow$	$\mathbb{Z}_{32} \times \mathbb{Z}_3$
$(4+1, 1)$ $\longrightarrow$	$\mathbb{Z}_{16} \times \mathbb{Z}_2 \times \mathbb{Z}_3$
$(3+2, 1)$ $\longrightarrow$	$\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_3$
$(3+1+1, 1)$ $\longrightarrow$	$\mathbb{Z}_8 \times (\mathbb{Z}_2)^2 \times \mathbb{Z}_3$
$(2+2+1, 1)$ $\longrightarrow$	$(\mathbb{Z}_4)^2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$
$(2+1+1+1, 1)$ $\longrightarrow$	$\mathbb{Z}_4 \times (\mathbb{Z}_2)^3 \times \mathbb{Z}_3$
$(1+1+1+1+1, 1)$ $\longrightarrow$	$(\mathbb{Z}_2)^5 \times \mathbb{Z}_3$

5) <u>Claim</u>: The map $\varphi: G/A \times A \to A$ $(gA \curvearrowright a)$

$$(gA, a) \mapsto gag^{-1}$$

is a well-defined group action.

1) Identity: $e \curvearrowright x = x$. Let $a \in A$, then

$$eA \curvearrowright a = eae^{-1} = a \in A. \checkmark$$

2) Composition: Let $g, h \in G \setminus A$, then

$$gA \curvearrowright (hA \curvearrowright a) = gA \curvearrowright (hah^{-1})$$

where $A \trianglelefteq G \Rightarrow gAg^{-1} = A$ and $h \in G, a \in A \Rightarrow hah^{-1} \in A$.

$$= g(hah^{-1})g^{-1}$$

$$= (gh)a(h^{-1}g^{-1})$$

$$= (gh)a(gh)^{-1}$$

$\in A$ since $gh \in G$ and $A \trianglelefteq G$.

$$= (gA \cdot hA) \curvearrowright a$$

$\leftarrow$ (Binary operation on cosets)

$$= ghA \curvearrowright a. \checkmark$$

3) Well-defined: Suppose $gA = hA$

Then $h^{-1}gA = A$, so $hg^{-1} \in A$. But then

$$h^{-1}gA \curvearrowright a = h^{-1}gag^{-1}h$$

$\in A$ since $h^{-1}g, g^{-1}h \in A$

$$= a$$

Since A is abelian

$$= eA \curvearrowright a$$

6) If $Z(G)=G$, then G is abelian and we are done.

Suppose $G/Z(G)$ is cyclic. Then $G/Z(G) = \langle tZ(G) \rangle$ for some $t \in G \cap Z(G)^c$. Now let $g,h \in G \cap Z(G)^c$; we want to show $gh=hg$. Let $\pi : G \twoheadrightarrow G/Z(G)$ be the canonical projection, so $\pi(g) = gZ(G)$ and $\pi(h) = hZ(G)$.

Since $G/Z(G)$ is generated by $tZ(G)$, there exist some j,k such that

$$gZ(G) = t^j Z(G) \quad \text{and} \quad hZ(G) = t^k Z(G)$$

so $$t^{-j} g Z(G) \in Z(G) \quad \text{and} \quad t^{-k} h Z(G) \in Z(G)$$

and thus there exist $c_1, c_2 \in Z(G)$ such that

$$t^{-j} g = c_1 \Rightarrow g = c_1 t^j$$
$$t^{-k} h = c_2 \Rightarrow h = c_1 t^k$$

But then

$$\begin{aligned} gh &= c_1 t^j c_2 t^k \\ &= c_1 c_2 t^j t^k && \text{Since } c_2 \in Z(G) \\ &= c_1 c_2 t^k t^j && \text{exponents commute} \\ &= c_2 t^k c_1 t^j && \text{Since } c_1 \in Z(G) \\ &= h\, g. \; \blacksquare \end{aligned}$$

---

(7) Let $H \trianglelefteq G$ with $\#H = p^k$, where $\#G = p^n m$ for some $n \geq k$. By Sylow 1, there exists a $P \in \mathrm{Syl}(p, G)$ where $\#P = p^n$ and $H \leq P$. Letting $P' \in \mathrm{Syl}(p, G)$ be arbitrary, by Sylow 2, $\exists g \in G$ such that $gPg^{-1} = P'$. Then,

$$H \leq P \Rightarrow \underset{\text{Since } H \trianglelefteq G}{H = gHg^{-1}} \leq gPg^{-1} = P', \text{ so } H \leq P'. \; \blacksquare$$

(8) By Sylow 3,

- $n_p \equiv 1 \mod p \Rightarrow n_p \in \{1, p+1, 2p+1, \cdots\}$
- $n_p \mid q \Rightarrow n_p \in \{1, q\}$ (since q is prime)

Since $1 < q < p < p+1$, this forces $n_p = 1$.

So there is a unique $P \in \mathrm{Syl}(p,G)$, where $P \trianglelefteq G$ and

$$[G:P] = |G/P| = |G|/|P| = p^n q/p^n = q. \qquad \blacksquare$$