1) Let $\sigma = (i_1\ i_2 \cdots i_m) \in S_n$ be a cycle, where $m \le n$, so we have $\boxed{i_j \overset{\sigma}{\longmapsto} i_{j+1 \bmod m}}$ * For each $1 \le j \le m$.

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 <u>single</u> 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

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

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

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

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

---

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

Let $\tau_{ij} = (i \ \ j) \in S_n$, so for $1 \le i, j \le n$ we have $i \xmapsto{\tau_{ij}} j$ and $\tau_{ij}^2 = id$, and let $A = \{\tau_{ij} \mid 1 \le i, j \le n\}$.

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

$$\underbrace{S_n = \langle A \rangle}_{\text{Claim 1}} \underbrace{\subseteq}_{\text{Claim 2}} \langle \sigma, \tau \rangle \underbrace{\subseteq}_{\substack{\text{Since } \sigma,\tau \in S_n \\ \text{which is closed} \\ \text{under products}}} S_n \implies \underbrace{\langle \sigma, \tau \rangle = S_n}_{\substack{\text{What we want} \\ \text{to show}}}$$

<u>Proof of claim 1</u>: 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 $1 \leq m \leq n$; 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 $2 \leq k \leq m$ 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:

Let $\tau_{ij} = \overbrace{(i\ \ j)}^{\text{wlog, } 1\le i<j<n} \in \langle A \rangle$; 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

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

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. ∎

4) Note that if $1 \leq n \leq 20$ then $n \in \{p, p^2, p^3, p^4, pq, p^2q\}$ for distinct primes p, q. So by cases:

$n=p$: G is cyclic and $\boxed{G \cong \mathbb{Z}_p.}$ Why? By Cauchy, G contains a cyclic subgroup $H \leq G$ where $\#H = p$. But this forces $H = G$.

$n=p^2$: Two possibilities, $\boxed{G \cong \mathbb{Z}_{p^2} \text{ or } G \cong \mathbb{Z}_p \times \mathbb{Z}_p,}$ by the classification theorem.

$n=p^3$: Three possibilities, $\boxed{G \cong \mathbb{Z}_{p^3},\ \mathbb{Z}_p \times \mathbb{Z}_{p^2},\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p}$

$n=p^4$: Four possibilities, $\boxed{G \cong \mathbb{Z}_{p^4},\ \mathbb{Z}_p \times \mathbb{Z}_{p^3},\ \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2},\ \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p.}$

$n=pq$: One possibility, $\boxed{G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}}$

$n=p^2q$: Two possibilities, $\boxed{G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_q,\ \mathbb{Z}_{p^2q}}$

All by the classification theorem

n	Groups	Case	# of groups
1	$\{e\}$	p	1
2	$\mathbb{Z}_2$	p	1
3	$\mathbb{Z}_3$	p	1
4	$\mathbb{Z}_4, \mathbb{Z}_2^2$	p^2	2
5	$\mathbb{Z}_5$	p	1
6	$\mathbb{Z}_6$	pq	1
7	$\mathbb{Z}_7$	p	1
8	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^3$	p^3	3
9	$\mathbb{Z}_9, \mathbb{Z}_3^2$	p^2	2
10	$\mathbb{Z}_{10}$	pq	1
11	$\mathbb{Z}_{11}$	p	1
12	$\mathbb{Z}_4 \times \mathbb{Z}_3, \mathbb{Z}_2^2 \times \mathbb{Z}_3$	p^2q	2
14	$\mathbb{Z}_{14}$	pq	1
15	$\mathbb{Z}_{15}$	pq	1
16	$\mathbb{Z}_{16}, \mathbb{Z}_8 \times \mathbb{Z}_2, \mathbb{Z}_4^2, \mathbb{Z}_2^4$	p^4	4
17	$\mathbb{Z}_{17}$	p	1
18	$\mathbb{Z}_{18}, \mathbb{Z}_3^2 \times \mathbb{Z}_2$	p^2q	2
19	$\mathbb{Z}_{19}$	p	1
20	$\mathbb{Z}_{20}, \mathbb{Z}_4 \times \mathbb{Z}_5$	p^2q	1

$\blacksquare$

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

$$= eA \curvearrowright a.$$

$\blacksquare$

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

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

so

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

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

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

$\blacksquare$

---

7. Let $H \trianglelefteq G$ with $\#H = p^k$ where $\#G = p^n m$ with $n \geq k$.

Let P be a Sylow p-subgroup, so $\#P = p^n$; we want to show $H \subseteq P$.

By Sylow 1, H is contained in some p-subgroup of G of order p^{k+1}, and thus inductively in some Sylow p-subgroup P'. But all Sylow p-subgroups are conjugate, so

$$\exists g \in G \text{ such that } gP'g^{-1} = P$$

But then

$$H \le P' \implies gHg^{-1} \le gP'g^{-1} = P,$$

and since H is normal in G, $H = gHg^{-1} \le P$.

Since P was arbitrary, H is in <u>every</u> $P \in Syl(p, G)$. ∎

---

8) By Sylow 3, we have

(1) $n_p \equiv 1 \mod p \implies n_p \in \{1, p+1, 2p+1, \dots\}$

(2) n_p divides $q \implies n_p \in \{1, q\}$ since q is prime.

But since $1 < q < p < p+1$, if $n_p = q = kp+1$ for any $k > 0$, then $q > p$, a contradiction. So $n_p = 1$.

So there is one Sylow p-subgroup P, which is normal by Sylow 2, and P is unique since $n_p = 1$. Moreover,

$$P \trianglelefteq G \implies [G:P] = |G/P| = |G|/|P| = p^n q / p^n = q. \quad ∎$$