20241110 MATH3301 NOTE 7[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Group Action

1.1 Motivation

Given a group G and a set X, we want to study the symmetries on X induced by G. The most general symmetry and the most trivial symmetry are described as follows:

Proposition 1.1. Let X be a set.
The permutation group $\mathrm{Perm}(X)$ acts on X in sense that:
(1) For all $g \in \mathrm{Perm}(X)$ and $x \in X$, there exists a unique $g * x = g(x) \in X$.
(2) For all $g, g' \in \mathrm{Perm}(X)$ and $x \in X$, $(gg') * x = g(g'(x)) = g * (g' * x)$.
(3) For all $x \in X$, the identity $e \in \mathrm{Perm}(X)$ maps x to x.

Proposition 1.2. Let X be a set.
The trivial group $\{e\}$ acts on X in sense that:
(1) For all $x \in X$, there exists a unique $e * x = e(x) = x \in X$.
(2) For all $x \in X$, $(ee) * x = x = e * (e * x)$.
(3) For all $x \in X$, the identity $e \in \{e\}$ maps x to x.

The most general symmetry is too complicated to study, and the most trivial symmetry is not interesting. We want to do something "intermediate".

Definition 1.3. (**Left Action**)
Let G be a group, and X be a set.
If $*$ is a map from $G \times X$ to X, such that:
(1) For all $g, g' \in G$ and $x \in X$, $(gg') * x = g * (g' * x)$.
(2) For all $x \in X$, the identity $e \in G$ maps x to x.
Then $*$ is a left action of G on X.

Proposition 1.4. Let G be a group, and X be a set.
If G acts on X, then the following map is a homomorphism:

$$\sigma : G \to \mathrm{Perm}(X), g \mapsto \ell_g(x) = g * x$$

Proof. We may divide our proof into two parts.
Part 1: For all $g, g' \in G$:

$$\ell_{gg'}(x) = (gg') * x = g * (g' * x) = \ell_g \ell_{g'}(x)$$

Hence, σ preserves composition.
Part 2: For all $g \in G$:

$$\ell_g^{-1} = \ell_{g^{-1}}$$

Hence, the bijective map $\ell_g \in \mathrm{Perm}(X)$, σ is well-defined.
Combine the two parts above, we've proven that σ is a homomorphism.
Quod. Erat. Demonstrandum. $\square$

Remark: *Notice that this map σ may not be injective. To solve this problem, we define the kernel of group action and consider the quotient.*

Definition 1.5. (**Kernel**)
Let G be a group, and X be a set.
If $*$ is a left action of G on X, then define the kernel of $*$ as:

$$\mathrm{Ker}(*) = \{g \in G : \forall x \in X, g * x = x\}$$

Proposition 1.6. Let G be a group, and X be a set.
If $*$ is a left action of G on X, then $\mathrm{Ker}(*)$ is normal in G.

Proof. We may divide our proof into four parts.
Part 1: $\forall x \in X, e * x = x \implies e \in \mathrm{Ker}(*)$.
Hence, $\mathrm{Ker}(*)$ contains the identity e.
Part 2: For all $g, g' \in G$:

$$\begin{aligned} g, g' \in \mathrm{Ker}(*) &\implies \forall x \in X, g * x = x \text{ and } g' * x = x \\ &\implies \forall x \in X, (gg') * x = g * (g' * x) = x \\ &\implies gg' \in \mathrm{Ker}(*) \end{aligned}$$

Hence, $\mathrm{Ker}(*)$ is closed under composition.
Part 3: For all $g \in G$:

$$\begin{aligned} g \in \mathrm{Ker}(*) &\implies \forall x \in X, g * x = x \\ &\implies \forall x \in X, g^{-1} * x = g^{-1} * (g * x) = (g^{-1}g) * x = x \\ &\implies g^{-1} \in \mathrm{Ker}(*) \end{aligned}$$

Hence, $\mathrm{Ker}(*)$ is closed under inverse.
Part 4: For all $g \in G$ and $s \in \mathrm{Ker}(*)$ and $x \in X$:

$$(gsg^{-1}) * x = g * (s * (g^{-1} * x)) = g * (g^{-1} * x) = (g * g^{-1}) * x = x$$

Hence, $gsg^{-1} \in \mathrm{Ker}(*)$, $\mathrm{Ker}(*)$ is closed under conjugation.
Combine the four parts above, we've proven that $\mathrm{Ker}(*)$ is normal in G.
Quod. Erat. Demonstrandum. $\square$

Proposition 1.7. Let G be a group, and X be a set.
If G acts on X, and $\tilde{G} = G/\mathrm{Ker}(*)$, the the following map is an embedding:

$$\tilde{\sigma} : \tilde{G} \to \mathrm{Perm}(X), \tilde{g} \mapsto \ell_g(x) = g * x$$

Proof. We may divide our proof into two parts.
Part 1: For all $g, g' \in G$:

$$\begin{aligned} \tilde{g} = \tilde{g}' &\implies \exists s \in \mathrm{Ker}(*), g = g's \\ &\implies \ell_g(x) = g * x = (g's) * x = g' * (s * x) = g' * x = \ell_{g'}(x) \end{aligned}$$

Hence, $\tilde{\sigma}$ is well-defined.
Part 2: For all $g, g' \in G$:

$$\ell_{gg'}(x) = (gg') * x = g * (g' * x) = \ell_g \ell_{g'}(x)$$

Hence, $\tilde{\sigma}$ preserves composition.
Part 3: For all $g \in G$:

$$\begin{aligned} \ell_g = \ell_e &\implies \forall x \in X, g * x = \ell_g(x) = \ell_e(x) = e * x = x \\ &\implies g \in \mathrm{Ker}(*) \end{aligned}$$

Hence, $\tilde{\sigma}$ is injective.
Combine the four parts above, we've proven that $\tilde{\sigma}$ is an embedding.
Quod. Erat. Demonstrandum. □

1.2 Homomorphism and Isomorphism

Given a group G, it may act on two set X, X' in two ways $*, *'$.
We would like to investigate those structure-preserving maps, i.e., homomorphisms.

Definition 1.8. (**Homomorphism**)
Let $* : G \times X \to X, *' : G \times X' \to X'$ be two left actions, and $\sigma : X \to X'$ be a function. If $\forall g \in G$ and $x \in X$, $\sigma(g * x) = g *' \sigma(x)$, then σ is a homomorphism.

Definition 1.9. (**Isomorphism**)
Let $* : G \times X \to X, *' : G \times X' \to X'$ be two left actions, and $\sigma : X \to X'$ be a homomorphism. If σ is bijective, then σ is an isomorphism.

Lemma 1.10. Let $* : G \times X \to X$ be a left action.
The identity map $e : X \to X, x \mapsto x$ is an isomorphism.

Proof. We may divide our proof into two parts.
Part 1: The identity function e is bijective.
Part 2: For all $g \in G$ and $x \in X$:

$$e(g * x) = g * x = g * e(x)$$

Hence, the identity map e preserves left action.
Combine the two parts above, we've proven that e is an isomorphism.
Quod. Erat. Demonstrandum. $\square$

Lemma 1.11. Let $* : G \times X \to X, *' : G \times X' \to X'$ be two left actions, and $\sigma : X \to X'$ be a function. If σ is an isomorphism, then σ^{-1} is an isomorphism.

Proof. We may divide our proof into two parts.
Part 1: σ is bijective implies σ^{-1} is bijective.
Part 2: For all $g \in G$ and $x' \in X'$:

$$\sigma^{-1}(g *' x') = \sigma^{-1}(g *' \sigma(\sigma^{-1}(x'))) = \sigma^{-1}(\sigma(g * \sigma^{-1}(x'))) = g * \sigma^{-1}(x')$$

Hence, σ^{-1} preserves left action.
Combine the two parts above, we've proven that σ^{-1} is an isomorphism.
Quod. Erat. Demonstrandum. $\square$

Lemma 1.12. Let $* : G \times X \to X, *' : G \times X' \to X', *'' : G \times X'' \to X''$ be three left actions, and $\sigma : X \to X', \sigma' : X' \to X''$ be two functions.
(1) If σ, σ' are homomorphisms, then $\sigma'\sigma$ is a homomorphism.
(2) If σ, σ' are isomorphisms, then $\sigma'\sigma$ is an isomorphism.

Proof. For all $g \in G$ and $x \in X$:

$$\sigma'\sigma(g * x) = \sigma'(g *' \sigma(x)) = g *'' \sigma'\sigma(x)$$

Hence, $\sigma'\sigma$ preserves left action. We can prove (2) by imposing bijectivity on (1).
Quod. Erat. Demonstrandum. $\square$

Proposition 1.13. Let $G = D_n$ be the dihedral group of a regular n-gon, and $X = \langle \zeta \rangle$ be the set vertices of a regular n-gon.
(1) For each $\zeta^k \in X$, the following function $*_k$ is a left action of G on X:

$$*_k : G \times X \to X, r^m *_k x = x\zeta^m \text{ and } r^m\sigma *_k x = \overline{x}\zeta^{m+2k}$$

(2) For each $\zeta^k, \zeta^{k'} \in X$, the following function $\phi_{k,k'}$ is an isomorphism.

$$\phi_{k,k'} : X(\text{with } *_k) \to X(\text{with } *_{k'}), x \mapsto x\zeta^{k'-k}$$

Proof. We may divide our proof into four parts.
Part 1: For all $x \in X$:

$$
\begin{aligned}
(r^m r^{m'}) *_k x = r^{m+m'} *_k x = x\zeta^{m+m'} = (x\zeta^m)\zeta^{m'} = r^m *_k (r^{m'} *_k x) \\
(r^m \sigma r^{m'}) *_k x = r^{m-m'}\sigma *_k x = \overline{x}\zeta^{m-m'+2k} = \overline{(x\zeta^{m'})}\zeta^{m+2k} = r^m\sigma *_k (r^{m'} *_k x) \\
(r^m r^{m'}\sigma) *_k x = r^{m+m'}\sigma *_k x = \overline{x}\zeta^{m+m'+2k} = (\overline{x}\zeta^{m'+2k})\zeta^m = r^m *_k (r^{m'}\sigma *_k x) \\
(r^m \sigma r^{m'}\sigma) *_k x = r^{m-m'} *_k x = x\zeta^{m-m'} = \overline{(\overline{x}\zeta^{m'+2k})}\zeta^{m+2k} = r^m\sigma *_k (r^{m'}\sigma *_k x)
\end{aligned}
$$

Hence, composition is compatible with $*_k$.
Part 2: For all $x \in X$:

$$e *_k x = r^0 *_k x = x\zeta^0 = x$$

Hence, the identity element $e \in G$ is compatible with $*$.
Part 3: For all $x \in X$:

$$
\begin{aligned}
\phi_{k,k'}(r^m *_k x) = \phi_{k,k'}(x\zeta^m) = x\zeta^{m+k'-k} = r^m *_{k'} (x\zeta^{k'-k}) = r^m *_{k'} \phi_{k,k'}(x) \\
\phi_{k,k'}(r^m\sigma *_k x) = \phi_{k,k'}(\overline{x}\zeta^{m+2k}) = \overline{x}\zeta^{m+k+k'} = r^m\sigma *_{k'} (x\zeta^{k'-k}) = r^m\sigma *_{k'} \phi_{k,k'}(x)
\end{aligned}
$$

Hence, $\phi_{k,k'}$ preserves left action.
Part 4: $\phi_{k,k'}$ has an inverse:

$$\phi_{k,k'}^{-1} = \phi_{k',k}$$

Hence, $\phi_{k,k'}$ is bijective.
Quod. Erat. Demonstrandum. □

1.3 More Concepts on Group Action

The kernel $\mathrm{Ker}(*)$ *of a left action* $* : G \times X \to X$ *reduces the redundancy of an action. We would like to generalize this idea, so we loosen our requirements.*

Definition 1.14. (**Stabilizer Subgroup**)
Let $* : G \times X \to X$ be a left action, and x be an element of X.
Define the x-stabilizer subgroup as:

$$G_x = \{g \in G : g * x = x\}$$

Definition 1.15. (**Fixed Point Subset**)
Let $* : G \times X \to X$ be a left action, and g be an element of G.
Define the g-fixed point subset as:

$$X_g = \{x \in X : g * x = x\}$$

Proposition 1.16. Let $* : G \times X \to X$ be a left action.
If the following subset of $G \times X$ is finite:

$$\mathbf{Fix} = \{(g, x) \in G \times X : g * x = x\}$$

Then the following equality holds:

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |X_g| = |\mathbf{Fix}|$$

Proof. We may divide our proof into two steps.
Step 1: Project **Fix** to X via the map $\pi_X : \mathbf{Fix} \to X, (g, x) \mapsto x$:

$$\sum_{x \in X} |G_x| = \sum_{x \in X} |G_x \times \{x\}| = \sum_{x \in X} |\pi_X^{-1}(\{x\})| = |\mathbf{Fix}|$$

Step 2: Project **Fix** to G via the map $\pi_G : \mathbf{Fix} \to G, (g, x) \mapsto g$:

$$\sum_{g \in G} |X_g| = \sum_{g \in G} |\{g\} \times X_g| = \sum_{g \in G} |\pi_G^{-1}(\{g\})| = |\mathbf{Fix}|$$

Quod. Erat. Demonstrandum. □

The above identity is not so interesting, let's introduce a more interesting one.

Proposition 1.17. Let $* : G \times X \to X$ be a left action.
$\sim: X \to X, x \sim x'$ if $\exists g \in G, x = g * x'$ is an equivalence relation.

Proof. We may divide our proof into three parts.
Part 1: For all $x \in X$:

$$\exists e \in G, x = e * x \implies x \sim x$$

Hence, $\sim$ is reflexive.
Part 2: For all $x, x' \in X$:

$$\begin{aligned} x \sim x' &\implies \exists g \in G, x = g * x' \\ &\implies \exists g^{-1} \in G, x' = (g^{-1} g) * x' = g^{-1} * (g * x') = g^{-1} * x \\ &\implies x' \sim x \end{aligned}$$

Hence, $\sim$ is symmetric.

Part 3: For all $x, x', x'' \in X$:

$$\begin{aligned} x \sim x' \text{ and } x' \sim x'' &\implies \exists g, g' \in G, x = g * x' \text{ and } x' = g' * x'' \\ &\implies \exists gg' \in G, x = g * x' = g * (g' * x'') = (gg') * x'' \\ &\implies x \sim x'' \end{aligned}$$

Hence, $\sim$ is transitive.
Combine the three parts together, we've proven that $\sim$ is an equivalence relation.
Quod. Erat. Demonstrandum. $\square$

Remark: *Note that we cannot mirror this relation to G, because the equation $x' = g * x$ involves only one group element g.*

Definition 1.18. (Orbit)
Let $* : G \times X \to X$ be a left action, and x be an element of X.
Define the x-orbit $G * x$ as the equivalence class of x under $\sim$.

Remark: *As a corollary, if X is finite, then:*

$$|X| = \sum_{\text{All Distinct Orbits}} |G * x|$$

We may define X_G as the G-fixed point subset, then:

$$|X| = |X_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x|$$

2 Class Equation

2.1 The Counting Formula

For certain left action $* : G \times X \to X$, G is a group, which has clear structure, and X is a set, which has no extra structure. We want to associate certain subset of X with certain structure of G, so it becomes easier to study such subset of X.

Proposition 2.1. Let $* : G \times X \to X$ be a left action,
and x be an element of X. The following function ϕ is well-defined and bijective.

$$\phi : G/G_x \to G * x, gG_x \mapsto g * x$$

This suggests:

$$[G : G_x] = |G * x|$$

Proof. For all $g, g' \in G$:

$$\begin{aligned} gG_x = g'G_x &\iff \exists s \in G_x, g = g's \\ &\iff g * x = (g's) * x = g' * (s * x) = g' * x \end{aligned}$$

Hence, the surjective function ϕ is well-defined and injective.
Quod. Erat. Demonstrandum. $\square$

Remark: *As we generalize kernel* $\mathrm{Ker}(*)$ *to stabilizer* G_x*, we lose normality.*
Hence, G/G_x *is not a group, so we are not allowed to apply Lagrange theorem further.*
By choosing different representatives, we get different stabilizer subgroups.
What is the relationship between them?

Proposition 2.2. Let $* : G \times X \to X$ be a left action,
x be an element of X, and g be an element of G.
The following function σ is an isomorphism:

$$\phi : G_x \to G_{g*x}, s \mapsto gsg^{-1}$$

Proof. We may divide our proof into three parts.
Part 1: For all $s \in G$:

$$\begin{aligned} s \in G_x &\implies s * x = x \\ &\implies (gsg^{-1}) * (g * x) = (gsg^{-1}g) * x = (gs) * x = g * (s * x) = g * s \\ &\implies gsg^{-1} \in G_{g*s} \end{aligned}$$

Hence, σ is well-defined.
Part 2: For all $s, s' \in G_x$:

$$\sigma(ss') = gss'g^{-1} = gsg^{-1}gs'g^{-1} = \sigma(s)\sigma(s')$$

Hence, σ preserves composition.
Part 3: σ has the following inverse:

$$\sigma^{-1} : G_{g*x} \to G_x, s' \mapsto g^{-1}s'g$$

Hence, σ is bijective.
Combine the three parts above, we've proven that σ is an isomorphism.
Quod. Erat. Demonstrandum. $\square$

Remark: *As a corollary,* G_x *is normal in* G *iff* $\forall g \in G, G_{g*x} = G_x$*.*

Proposition 2.3. Consider the following subgroup G of S_6:

$\circ$	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_2	τ_3	τ_1
σ_2	σ_2	e	σ_1	τ_3	τ_1	τ_2
τ_1	τ_1	τ_3	τ_2	e	σ_2	σ_1
τ_2	τ_2	τ_1	τ_3	σ_1	e	σ_2
τ_3	τ_3	τ_2	τ_1	σ_2	σ_1	e

Here, the elements $e, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3$ are the following permutations:

$$\begin{aligned} e &= e \\ \sigma_1 &= (1,3,5)(2,6,4) \\ \sigma_2 &= (1,5,3)(2,4,6) \\ \tau_1 &= (1,2)(3,4)(5,6) \\ \tau_2 &= (2,3)(4,5)(6,1) \\ \tau_3 &= (1,4)(2,5)(3,6) \end{aligned}$$

(1) The group G acts on the set $X = \{1,2,3,4,5,6\}$ transitively.
(2) The stabilizer subgroups $G_1 = G_2 = G_3 = G_4 = G_5 = G_6$ are trivial.
(3) The center of the quotient group $G/\{e\} \cong S_3$ is trivial.

Remark: *If $\ell_s : X(\text{with } *) \to X(\text{with } *), x \mapsto s * x$ is an isomorphism, then:*

$$\forall g \in G \text{ and } x \in X, \ell_s(g * x) = g * \ell_s(x)$$

As the kernel $\mathrm{Ker}(*)$ is trivial, this is equivalent to saying s is in the center of G.
As the center of $G/\{e\}$ is trivial, the element s must be the identity e.
That is to say, applying ℓ_s to X, where $s \neq e$, breaks the structure of this action.

2.2 Class Equation

Proposition 2.4. Let G be a finite group, and X be a finite set.
If G acts on X, then we have:

$$|X| = |X_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G|/|G_x|$$

Proof.

$$\begin{aligned}|X| &= |X_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x| \\ &= |X_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} [G : G_x] \\ &= |X_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G|/|G_x|\end{aligned}$$

Quod. Erat. Demonstrandum. ☐

Lemma 2.5. Let G be a group, N be a normal subgroup of G.
(1) The following function $*$ is a left action of G on N:

$$* : G \times N \to N, g * n = gng^{-1}$$

(2) The G-fixed point subset $N_G = Z_G \cap N$, where Z_G is the center of G.

Proof. We may divide our proof into three parts.
Part 1: For all $g \in G$ and $x \in N$, as N is normal in G, $gxg^{-1} \in N$.
Hence, $*$ is a well-defined function.
Part 2: For all $g, g' \in G$ and $x \in N$:

$$(gg') * x = (gg')x(gg')^{-1} = gg'xg'^{-1}g^{-1} = g * (g' * x)$$

Hence, $*$ is compatible with composition.
Part 3: For all $x \in N$:

$$e * x = exe^{-1} = x$$

Hence, $*$ is compatible with the identity element $e \in G$.
Part 4: For all $x \in N$:

$$x \in N_G \iff \forall g \in G, g * x = gxg^{-1} = x \iff \forall g \in G, gx = xg \iff x \in Z_G \cap N$$

Hence, the G-fixed point subset $N_G = Z_G \cap N$, where Z_G is the center of G.
Quod. Erat. Demonstrandum. ☐

Proposition 2.6. Let G be a finite group. We have:

$$|G| = |Z_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x|$$

Proof. Consider the left action described in **Lemma 2.5.** with $N = G$.

$$\begin{aligned}|G| &= |N_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x| \\ &= |Z_G \cap N| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x| \\ &= |Z_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x|\end{aligned}$$

Quod. Erat. Demonstrandum. $\square$

Proposition 2.7. Let G be a finite group with odd order, and N be a normal subgroup of G with order 5. N is contained in the center Z_G of G.

Proof. We may prove this fact step by step.
(1) Consider the left action described in **Lemma 2.5.**.
(2) Assume to the contrary that N has at least one nonsingleton orbit $G * \xi$.
(3) As $|G * \xi| = |G|/|G_\xi| \geq 3$, the following class equation implies $|Z_G \cap N| = 2$:

$$|N| = |Z_G \cap N| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x|$$

(4) However, the order of G, which is odd, is not divisible by the order of $Z_G \cap N$, which is even, contradicting to Lagrange's theorem.
(5) Hence, our assumption is false, and we get the following degenerate equation:

$$|N| = |Z_G \cap N|$$

(6) The equation above suggests that N is contained in the center Z_G of G.
Quod. Erat. Demonstrandum. $\square$

3 Sylow Theorems

3.1 Group with Few Prime Factors

The first interesting group with few prime factors is p-group.

Definition 3.1. (p**-group**)
Let G be a group, $p \geq 2$ be a prime number, and $n \geq 1$ be an integer.
If the order of G is $|G| = p^n$, then G is a p-group.

Proposition 3.2. If G is a p-group, then the center Z_G of G is nontrivial.

Proof. Consider the class equation:

$$|G| = |Z_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x|$$

Note that $|G * x|$ is a nontrivial factor of $|G| = p^n$, so $|Z_G|$ must be a multiple of p.
Note that $e \in Z_G$, so $|Z_G| \geq p$, $|Z_G|$ is nontrivial. Quod. Erat. Demonstrandum. $\square$

Remark: *S_3 is not a p-group, and S_3 has a trivial center.*
D_4 is a 2-group, and D_4 has a nontrivial center $\{e, r^2\}$.

Proposition 3.3. Let G be a group, and $p \geq 2$ be a prime number.
If the order of G is p^2, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. We wish to prove that G is Abelian, then the result follows from the classification theorem for finite Abelian groups. Assume to the contrary that G is nonAbelian.
There exists an element $g \in G$, such that the centralizer subgroup $C_{\langle g \rangle}$ is proper in G.
This centralizer subgroup $C_{\langle g \rangle}$ contains the center Z_G, so $|C_{\langle g \rangle}| \geq |Z_G| \geq p$.
This centralizer subgroup $C_{\langle g \rangle}$ contains one more element g than Z_G, so $|C_{\langle g \rangle}| > p$.
Hence, the index $[G : C_{\langle g \rangle}] = 1$, and we get a contradiction where $g \in Z_G$ and $g \notin Z_G$.
To conclude, we've proven that G is Abelian. Quod. Erat. Demonstrandum. $\square$

Remark: *As $|D_4| = 2^3$ and D_4 is nonAbelian, the assumption $|G| = p^2$ is necessary.*

Proposition 3.4. Let G be a group, and $p, q \geq 2$ be two prime numbers.
If the order of G is pq, and there exist normal subgroups P, Q of G with $|P| = p$ and $|Q| = q$, then G is Abelian.

Proof. WLOG, assume that $p \neq q$.
Note that $P \cap Q$ must be trivial, so $|HK| = |H||K| = pq = |G|$.
Assume that the cyclic groups P, Q have generators x, y respectively.
As P is normal in G, for some $0 \leq n < p$, $yxy^{-1} = x^{n+1}$.
As Q is normal in G, for some $0 \leq m < q$, $xyx^{-1} = y^{m+1}$.
As $x^n y^m = yxy^{-1}x^{-1}xyx^{-1}y^{-1} = e$, both x^n and y^m lie in $P \cap Q$, so $xy = yx$.
Quod. Erat. Demonstrandum. $\square$

Remark: *Consider a group G of order 6.*
If G is Abelian, then $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.
If G is nonAbelian, then we cannot simultaneously find two normal subgroups P, Q of G, such that $|P| = 2$ and $|Q| = 3$. For $G = S_3$, P fails to exist.

3.2 Sylow's First Theorem

Definition 3.5. (p**-Sylow Subgroup**)
Let G be a group, $p \geq 2$ be a prime number,
and $n \geq 0, m \geq 1$ be two integers.
If the order of G is $|G| = p^n m$ and $p \nmid m$,
then every subgroup H of G with order $|H| = p^n$,
if exists, is a p-Sylow subgroup of G.

Remark: *In* D_4, $\{e\}, \{e, \sigma\}, \{e, r^2\}, \{e, r, r^2, r^3\}, \{e, r^2, \sigma, r^2\sigma\}, D_4$ *are* 2*-subgroups of* D_4*, and* D_4 *is a* 2*-Sylow subgroup of* D_4.
In S_4*, any embedding of* D_4 *is a* 2*-Sylow subgroup of* S_4*, where* $|D_4| = 2^3 \| 4! = |S_n|$.
In S_4*, any embedding of* $\mathbb{Z}_3$ *is a* 3*-Sylow subgroup of* S_4*, where* $|\mathbb{Z}_3| = 3^1 \| 4! = |S_n|$.

Lemma 3.6. Let $p \geq 2$ be a prime number.
The following relation $\prec_p$ on $\mathbb{N}$ is a total order:
(1) If $\max\{n \geq 0 : p^n | l\} > \max\{n \geq 0 : p^n | l'\}$, then $l \not\prec_p l'$.
(2) If $\max\{n \geq 0 : p^n | l\} < \max\{n \geq 0 : p^n | l'\}$, then $l \prec_p l'$.
(3) If $\max\{n \geq 0 : p^n | l\} = \max\{n \geq 0 : p^n | l'\}$ and $l \geq l'$, then $l \not\prec_p l'$.
(4) If $\max\{n \geq 0 : p^n | l\} = \max\{n \geq 0 : p^n | l'\}$ and $l < l'$, then $l \prec_p l'$.

Remark: *This total order on* $\mathbb{N}$ *is different from the usual order on* $\mathbb{N}$ *because* $11 \prec_2 2$.
Our proof to Sylow's first theorem is organized according to $\prec_p$.

Theorem 3.7. (**Sylow's First Theorem**[2])
Let G be a group, and $p \geq 2$ be a prime number. G has a p-Sylow subgroup.

Proof. We may divide our proof into three parts.
Part 1: The theorem holds trivially when $|G| \prec_p p$.
Part 2: The theorem holds trivially when $|G|$ is a power of p.
Part 3: For all $n \geq 1$, we wish to prove the following implication:

$$[\text{The theorem holds for all } |G| \prec_p p^n] \implies [\text{The theorem holds for all } |G| \prec_p p^{n+1}]$$

As the theorem is true when $|G| \preceq_p p^n$, it suffices to consider the case $p^n \prec_p |G| \prec_p p^{n+1}$.
Case 3.1: If p^n divides some $|G_x|$, where G_x is a proper stabilizer subgroup of G, then:
(1) Replace G by G_x and repeat the algorithm, until no such G_x is found.
(2) If $|G|$ is reduced to p^n, then go to **Part 2.**.
(3) If $|G|$ is not reduced to p^n, then go to **Case 3.2.**.
Case 3.2: If p^n divides no $|G_x|$, where G_x is a proper stabilizer subgroup of G, then:
(1) $|G|$ and each $|G * x|$ are multiples of p.

(2) The following class equation suggests $|Z_G|$ is a multiple of p:

$$\begin{aligned}|G| &= |Z_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G * x| \\ &= |Z_G| + \sum_{\text{All Distinct Nonsingleton Orbits}} |G|/|G_x|\end{aligned}$$

(3) As Z_G is an Abelian group with a prime divisor p, Cauchy's theorem for Abelian group suggests the existence of an element $\xi \in Z_G$ of order p.
(4) Now the quotient group $G/\langle\xi\rangle$ is well-defined and $|G/\langle\xi\rangle| = |G|/p \prec_p p^n$.
(5) The inductive hypothesis suggests the existence of a p-Sylow subgroup $\tilde{P}$ of $G/\langle\xi\rangle$.
(6) Consider the preimage P of $\tilde{P}$ under the natural projection map $\pi : G \to \tilde{G} = G/\langle\xi\rangle, x \mapsto \tilde{x}$. As $|P| = |\tilde{P}||\mathrm{Ker}(\pi)| = p^{n-1}p = p^n$, P is a p-Sylow subgroup of G.
Combine the two parts above, we've proven Sylow's first theorem.
Quod. Erat. Demonstrandum. □

Remark: *Cauchy's theorem follows as an easy corollary of Sylow's first theorem.*

Theorem 3.8. (**Cauchy's Theorem**[2])
Let G be a group, and $p \geq 2$ be a prime number.
If p divides the order $|G|$ of G, then G has an element ξ of order p.

Proof. Take a p-Sylow subgroup P of G.
As p divides the order $|G|$ of G, P contains a nontrivial element ξ.
Assume that $\mathrm{Ord}(\xi) = p^r$, where r is a positive integer.
Now $\mathrm{Ord}(\xi^{p^{r-1}}) = \mathrm{Ord}(\xi)/p^{r-1} = p^r/p^{r-1} = p$, and we are done.
Quod. Erat. Demonstrandum. □

3.3 Sylow's Second Theorem

Lemma 3.9. Let $* : G \times X \to X$ be a left action, and $p \geq 2$ be a prime number.
If G is a p-group, and p doesn't divide the cardinality $|X|$ of X,
then the G-fixed point subset X_G is nonempty.

Proof. Consider the orbit decomposition formula:

$$\begin{aligned}|X| &= |X_G| + \sum_{\text{All Distinct Nonsingleton Orbit}} |G * x| \\ &= |X_G| + \sum_{\text{All Distinct Nonsingleton Orbit}} |G|/|G_x|\end{aligned}$$

As each $|G*x| = |G|/|G_x|$ is a multiple of p, $p \nmid |X|$ implies $p \nmid |X_G|$, so X_G is nonempty.
Quod. Erat. Demonstrandum. □

Remark: *The existence of a G-fixed point helps to prove Sylow's second theorem.*

Lemma 3.10. Let G be a group, and H, Q be two subgroups of G.
If H is contained in the normalizer subgroup of Q,
then Q is normal in HQ and $H \cap Q$ is normal in H.

Proof. We check the key properties one by one.
(1) Q is assumed to be a subgroup of G, so Q is a group.
(2) H is assumed to be a subgroup of G, so H is a group.
(3) H, Q are two subgroups of G, so $H \cap Q$ is a subgroup of G, $H \cap Q$ is a group.
(4) H is contained in the normalizer subgroup of Q, so HQ is a group.
(5) $Q \leq HQ$, and for all $hq \in HQ$, $hqQ = hQq = Qhq$, so Q is normal in HQ.
(6) $H \cap Q \leq H$, and for all $h \in H$, $h(H \cap Q) = hH \cap hQ = Hh \cap Qh = (H \cap Q)h$, so $H \cap Q$ is normal in H. Quod. Erat. Demonstrandum. □

Remark: *In this situation, it is allowed to apply the second isomorphism theorem:*

$$H/(H \cap Q) \cong (HQ)/Q$$

Theorem 3.11. (**Sylow's Second Theorem**[3])
Let G be a group, and $p \geq 2$ be a prime number.
Every p-subgroup is contained in a p-Sylow subgroup.

Proof. Let P be a p-Sylow subgroup of G found by Sylow's first theorem.
For all p-subgroup H of G, we wish to find a conjugate of P, such that $H \leq P$.
Step 1: We construct a special conjugate Q of P.
(1) Consider the set $\mathbf{P}$ of all p-Sylow subgroups of G.
Any subgroup of G acts on $\mathbf{P}$ by conjugation.
(2) Consider the P-stabilizer subgroup G_P of G.
As $P \leq G_P \leq G$, the number $[G : G_P] = |G * P|$ is not divisible by p.
(3) Consider the orbit $G * P$ of P under conjugation.
G acts on $G * P$ implies the subgroup H of G acts on $G * P$.
(4) As H is a p-group, and p doesn't divide the cardinality $|G * P|$ of $G * P$,
Lemma 3.9. suggests the G-fixed point subset $(G * P)_H$ is nonempty.
(5) Take a conjugate $Q = gPg^{-1} \in (G * P)_H$,
H is contained in the normalizer subgroup of Q.
Step 2: We prove that H is contained in this conjugate Q of P.
(1) As H, Q are subgroups of G, and H is contained in the normalizer subgroup of Q,
Lemma 3.10. suggests that we are allowed to apply the second isomorphism theorem.

$$H/(H \cap Q) \cong (HQ)/Q$$

(2) The above isomorphism implies $|HQ| = |Q||H/(H \cap Q)|$.
(3) As H is a p-group, its quotient $H/(H \cap Q)$ is also a p-group.
(4) As both Q and $H/(H \cap Q)$ are p-groups, HQ is also a p-group.

(5) As Q is a p-Sylow subgroup of G, the order $|HQ| \geq |Q|$ of the p-group $HQ \supseteq Q$ cannot exceed $|Q|$, so $|HQ| = |Q|$, which implies $HQ = Q$ and $H \subseteq Q$.
Quod. Erat. Demonstrandum. $\square$

Remark: *Since new p-Sylow subgroups are constructed by conjugation, G acts transitively on the set of all p-Sylow subgroups by conjugation.*

Proposition 3.12. Let G be a group, and $p \geq 2$ be a prime number.
If the p-Sylow subgroup P of G is unique, then P is normal in G.

Proof. Consider the set $\mathbf{P}$ of all p-Sylow subgroups of G. Sylow's second theorem suggests that $\mathbf{P} = G * P$ is a single orbit, and the orbit is a singleton suggests P is normal in G. Quod. Erat. Demonstrandum. $\square$

Proposition 3.13. Let G be a group, and $p \geq 2$ be a prime number.
If p divides the order $|G|$ of G and G is simple and G is not a p-group,
then $|G|$ divides $r_p!$, where r_p is the number of p-Sylow subgroups of G.

Proof. We may prove this fact step by step.
(1) Consider the left action $* : G \times \mathbf{P} \to \mathbf{P}, g * P = gPg^{-1}$.
(2) As G is simple, $\mathrm{Ker}(*) = \{e\}$ or $\mathrm{Ker}(*) = G$.
(3) To further prove that $\mathrm{Ker}(*) = \{e\}$, fix a p-Sylow subgroup P of G.
(4) As p divides $|G|$ and G is not a p-group, P is a nontrivial proper subgroup of G.
(5) As G is simple, the nontrivial proper subgroup P of G is not normal in G.
(6) **Proposition 3.12.** suggests that some $g * P = gPg^{-1} \neq P$.
(7) Hence, $\mathrm{Ker}(*)$ misses at least one element g of G, $\mathrm{Ker}(*)$ must be $\{e\}$.
(8) **Proposition 1.7.** suggests that $G \cong G/\mathrm{Ker}(*)$ is embedded in $\mathrm{Perm}(\mathbf{P}) \cong S_{r_p}$.
(9) Lagrange's theorem implies that $|G|$ divides $|S_{r_p}| = r_p!$.
Quod. Erat. Demonstrandum. $\square$

3.4 Sylow's Third Theorem

Theorem 3.14. (**Sylow's Third Theorem**[3])
Let G be a group, and $p \geq 2$ be a prime number. The number r_p of p-Sylow subgroups of G divides the order $|G|$ of G, and $r_p \equiv 1 (\mathrm{mod}\ p)$.

Proof. We may divide our proof into two parts.
Part 1: We prove that r_p divides the order $|G|$ of G.
Consider the set $\mathbf{P}$ of all p-Sylow subgroups of G. Sylow's second theorem suggests that $\mathbf{P} = G * P$ is a single orbit, so $r_p = |G * P| = |G|/|G_P|$ divides the order $|G|$ of G.
Part 2: We prove that $r_p \equiv 1 (\mathrm{mod}\ p)$.

Fix $H \in \mathbf{P}$. The group H acts on $\mathbf{P}$ by conjugation.
Consider the orbit decomposition formula:

$$\begin{aligned}|\mathbf{P}| &= |\mathbf{P}_H| + \sum_{\text{All Distinct Nonsingleton Orbits}} |H * P| \\ &= |\mathbf{P}_H| + \sum_{\text{All Distinct Nonsingleton Orbits}} |H|/|H_P|\end{aligned}$$

For all nonsingleton orbit $H * P$, $|H * P| = |H|/|H_P|$ is a multiple of p,
so it suffices to prove $\mathbf{P}_H = \{H\}$. As $H \in \mathbf{P}_H$, we proceed to prove $\mathbf{P}_H \subseteq \{H\}$.
For all $Q \in \mathbf{P}_H$, H is contained in the normalizer of P.
Quote **Lemma 3.10.** again, and we get the following isomorphism:

$$H/(H \cap P) \cong (HP)/P$$

For the same reason in the proof of Sylow's second theorem,
$|H/(H \cap P)|$ must be trivial, so H is a subgroup of P.
As $H \leq P$ and $|H| = |P|$, $H = P$, and we are done.
Quod. Erat. Demonstrandum. □

Remark: *If we write $|G|$ in the form $p^n m$, where $p \nmid m$, then $r_p | m$.*

Proposition 3.15. Let G be a group, and $p, q \geq 2$ be two prime numbers.
If $|G| = pq$ and $p \nmid q - 1$ and $q \nmid p - 1$, then G is Abelian.

Proof. We may divide our proof into three steps.
Step 1: As $r_p | q$ and $p | r_p - 1$ and $p \nmid q - 1$, it must be true that $r_p = 1$.
Proposition 3.12. suggests that the unique p-Sylow subgroup P of G is normal in G.
Step 2: As $r_q | p$ and $q | r_q - 1$ and $q \nmid p - 1$, it must be true that $r_q = 1$.
Proposition 3.12. suggests that the unique q-Sylow subgroup Q of G is normal in G.
Step 3: As $|G| = pq$ and $|P| = p$ and $|Q| = q$ and P, Q are normal in G,
Proposition 3.4. suggests that G is Abelian. Quod. Erat. Demonstrandum. □

Remark: *It follows that a group of order $143 = 11 * 13$ must be cyclic.*
This is almost impossible to prove by brute force!

4 The Alternating Group A_n

4.1 Preliminaries

Proposition 4.1. Let X, X' be two sets, and $f : X \to X'$ be a bijection.
$c_f : \mathrm{Perm}(X) \to \mathrm{Perm}(X'), \sigma \mapsto f\sigma f^{-1}$ is an isomorphism.

Proof. We may divide our proof into three parts.
Part 1: For all $\sigma : X \to X$:

$$\sigma \in \mathrm{Perm}(X) \implies \sigma \text{ is bijective} \implies f\sigma f^{-1} \text{ is bijective} \implies f\sigma f^{-1} \in \mathrm{Perm}(X')$$

Hence, c_f is well-defined.
Part 2: Note that c_f has the following inverse:

$$c_f^{-1} : \mathrm{Perm}(X') \to \mathrm{Perm}(X), \sigma' \mapsto f^{-1}\sigma' f$$

Hence, c_f is bijective.
Part 3: For all $\sigma_1, \sigma_2 \in \mathrm{Perm}(X)$:

$$c_f(\sigma_1\sigma_2) = f\sigma_1\sigma_2 f^{-1} = f\sigma_1 f^{-1} f\sigma_2 f^{-1} = c_f(\sigma_1)c_f(\sigma_2)$$

Hence, c_f preserves composition.
To conclude, c_f is an isomorphism. Quod. Erat. Demonstrandum. $\square$

Remark: *Hence, we can define symmetric group with a given cardinality.*

Definition 4.2. (**The Symmetric Group S_n**)
Let n be a positive integer. Choose a set X with cardinality n.
Define the symmetric group S_n as the permutation group $\mathrm{Perm}(X)$.

Definition 4.3. (**Cycle and Transposition**)
Let σ be an element of $\mathrm{Perm}(X)$.
If there exists $k \geq 1$ distinct elements $x_1, x_2, \cdots, x_{k-1}, x_k$ of X, such that:

$$\sigma(x) = \begin{cases} x_{l+1} & \text{if} \quad x \text{ is equal to some } x_l \quad \text{and} \quad 1 \leq l < k; \\ x_1 & \text{if} \quad x \text{ is equal to some } x_l \quad \text{and} \quad l = k; \\ x & \text{if} \quad x \text{ is equal to no } x_l; \end{cases}$$

Then, $\sigma = (x_1, x_2, \cdots, x_{k-1}, x_k)$ is a k-cycle.
Especially, if $k = 2$, then (x_1, x_2) is a transposition.

Definition 4.4. (**Disjoint Permutation**)
Let σ_1, σ_2 be two elements of $\mathrm{Perm}(X)$.
If for all $x_1, x_2 \in X$, $\sigma_1(x_1) = x_1$ or $\sigma_2(x_2) = x_2$, then σ_1 and σ_2 are disjoint.

Lemma 4.5. Let σ be an element of the symmetric group S_n.
σ is a cycle or a finite product of pairwisely disjoint cycles.

Proof. We prove this theorem by the strong form of mathematical induction.
Step 1: When $n = 1$, $\sigma = e$ is a 1-cycle, the statement holds.

Step 2: For all $m \in \mathbb{N}$, when $n = 1, 2, \cdots, m$, assume that the statement holds.
Step 3: When $n = m + 1$, there are two cases to consider.
Case 3.1: If σ is a cycle, then we are done.
Case 3.2: If σ is not a cycle, then:
(1) Fix an arbitrary $\xi \in X$.
(2) For some $1 \leq l < m + 1$, the orbit $\langle\sigma\rangle * \xi = \{\xi, \sigma(\xi), \sigma^2(\xi), \cdots, \sigma^{l-1}(\xi)\}$.
(3) If $\sigma|_{(\langle\sigma\rangle*\xi)^c}$ is a cycle σ_1 in S_{m+1-l},
then $\sigma = \sigma_1(\xi, \sigma(\xi), \cdots, \sigma^{l-1}(\xi))$ is a product of cycles in S_{m+1}.
(4) If $\sigma|_{(\langle\sigma\rangle*\xi)^c}$ is a product of pairwisely disjoint cycles $\sigma_1 \cdots \sigma_k$ in S_{m+1-l},
then $\sigma = \sigma_1 \cdots \sigma_k(\xi, \sigma(\xi), \cdots, \sigma^{l-1}(\xi))$ is a product of cycles in S_{m+1}.
(5) As $\langle\sigma\rangle * \xi$ and $(\langle\sigma\rangle * \xi)^c$ are disjoint,
$\sigma_1, \cdots, \sigma_k, (\xi, \sigma(\xi), \cdots, \sigma^{l-1}(\xi))$ are pairwisely disjoint.
Hence, we've proven the statement. Quod. Erat. Demonstrandum. ☐

Remark: *Actually this representation is unique under arrangement, because the orbit $\langle\sigma\rangle * x$ of each $x \in X$ is unique.*

Lemma 4.6. When $n \geq 2$, each $\sigma \in S_n$ is a finite product of 2-cycles.

Proof. Assume that all distinct elements of X are $x_1, x_2, \cdots, x_n$.
Case 1: If $\sigma = e$, then $e = (x_1, x_2)(x_1, x_2)$ is a finite product of 2-cycles.
Case 2: If $\sigma \neq e$, then find the smallest $1 \leq k \leq n$ such that $\sigma(x_k) \neq x_k$.
Consider the product $(x_k, \sigma(x_k))\sigma$.
Situation 2.1: If $(x_k, \sigma(x_k))\sigma = e$, then $\sigma = (x_k, \sigma(x_k))$ is a 2-cycle.
Situation 2.2: If $(x_k, \sigma(x_k))\sigma \neq e$, then define $\tau = (x_k, \sigma(x_k))\sigma$ and repeat.
This process eventually ends because there are finitely many elements to permute.
Hence, $\sigma = (x_k, \sigma(x_k))\tau$ is a finite product of 2-cycles.
Quod. Erat. Demonstrandum. ☐

Lemma 4.7. Let N be a normal subgroup of $\mathrm{Perm}(X)$.
If N contains a transposition, then N contains all transpositions.

Proof. Assume that N contains a transposition (ξ_1, ξ_2).
Now for all transposition (x_1, x_2):
Case 1: (x_1, x_2) and (ξ_1, ξ_2) have 2 common entries.
In this case, $(x_1, x_2) = (\xi_1, \xi_2) \in N$.
Case 2: (x_1, x_2) and (ξ_1, ξ_2) have 1 common entry.
In this case, WLOG, assume that $x_1 = \xi_1$ and $x_2 \neq \xi_2$,
so $(x_1, x_2) = (x_2, \xi_2)(\xi_1, \xi_2)(x_2, \xi_2)^{-1} \in N$.
Case 3: (x_1, x_2) and (ξ_1, ξ_2) have 0 common entry.
In this case, $(x_1, x_2) = [(x_1, \xi_1)(x_2, \xi_2)](\xi_1, \xi_2)[(x_1, \xi_1)(x_2, \xi_2)]^{-1} \in N$.
Hence, N contains all transpositions. Quod. Erat. Demonstrandum. ☐

Proposition 4.8. In the symmetric group S_n,
a unique maximal proper normal subgroup A_n exists.

Proof. We may divide our proof into two parts.
Part 1: In this part, we prove the existence of A_n.
Define $\text{Spec}(S_n)$ as the set of all proper normal subgroups of S_n.
We wish to find a maximal element A_n of $\text{Spec}(S_n)$.
Assume to the contrary that such element fails to exist.
There exists a sequence of normal subgroups $(H_m)_{m\in\mathbb{N}}$ of S_n, such that:

$$\forall m \in \mathbb{N}, H_m \subset H_{m+1}$$

But S_n is finite, it cannot have an infinite strictly increasing sequence.
Hence, there exists $A_n \in \text{Spec}(S_n)$, such that for all $H \in \text{Spec}(S_n)$:

$$A_n \subseteq H \implies A_n = H$$

Part 2: In this part, we prove the uniqueness of A_n.
For all transposition (x_1, x_2), as A_n is maximal,
the smallest normal subgroup of S_n containing $A_n \cup \{(x_1, x_2)\}$ is S_n.
Hence, $S_n = A_n \sqcup (x_1, x_2)A_n$.
For all transpositions $(x_1, x_2), (x_1', x_2')$:

$$(x_1, x_2)A_n = (x_1', x_2')A_n = A_n^c \implies (x_1, x_2)(x_1', x_2') \in A_n$$

This implies:
(1) All even product of transpositions is contained in A_n.
(2) All odd product of transpositions is contained in A_n^c.
As the two types of products partition S_n, A_n is unique.
Quod. Erat. Demonstrandum. ☐

Definition 4.9. (**The Alternating Group** A_n)
When $n \geq 2$, define A_n as the unique maximal proper normal subgroup of S_n.

4.2 A_2, A_3 Are Simple

Proposition 4.10. A_2, A_3 are simple.

Proof. Note that $A_2 = \langle e \rangle$ is trivial and $A_3 \cong \mathbb{Z}_3$ is prime, so both of them are simple.
Quod. Erat. Demonstrandum. ☐

4.3 A_4 Is Not Simple

Proposition 4.11. A_4 is not simple.

Proof. For simplicity, take $X = \{1, 2, 3, 4\}$. Consider the following subset K_4 of A_4:

$$K_4 = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

Step 1: We show that K_4 is a group.

$\circ$	e	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
e	e	$(1,2)(3,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$
$(1,2)(3,4)$	$(1,2)(3,4)$	e	$(1,4)(2,3)$	$(1,3)(2,4)$
$(1,3)(2,4)$	$(1,3)(2,4)$	$(1,4)(2,3)$	e	$(1,2)(3,4)$
$(1,4)(2,3)$	$(1,4)(2,3)$	$(1,3)(2,4)$	$(1,2)(3,4)$	e

Step 2: By direct computation, we can show that K_4 is normal in S_4, so in A_4.

σ	σK_4	$K_4\sigma$
e	$\left\{\begin{matrix} e & (1,2)(3,4) \\ (1,3)(2,4) & (1,4)(2,3) \end{matrix}\right\}$	$\left\{\begin{matrix} e & (1,2)(3,4) \\ (1,3)(2,4) & (1,4)(2,3) \end{matrix}\right\}$
$(1,2)$	$\left\{\begin{matrix} (1,2) & (3,4) \\ (1,3,2,4) & (1,4,2,3) \end{matrix}\right\}$	$\left\{\begin{matrix} (1,2) & (3,4) \\ (1,4,2,3) & (1,3,2,4) \end{matrix}\right\}$
$(1,3)$	$\left\{\begin{matrix} (1,3) & (1,2,3,4) \\ (2,4) & (1,4,3,2) \end{matrix}\right\}$	$\left\{\begin{matrix} (1,3) & (1,4,3,2) \\ (2,4) & (1,2,3,4) \end{matrix}\right\}$
$(1,4)$	$\left\{\begin{matrix} (1,4) & (1,2,4,3) \\ (1,3,4,2) & (2,3) \end{matrix}\right\}$	$\left\{\begin{matrix} (1,4) & (1,3,4,2) \\ (1,2,4,3) & (2,3) \end{matrix}\right\}$
$(1,2,3)$	$\left\{\begin{matrix} (1,2,3) & (1,3,4) \\ (2,4,3) & (1,4,2) \end{matrix}\right\}$	$\left\{\begin{matrix} (1,2,3) & (2,4,3) \\ (1,4,2) & (1,3,4) \end{matrix}\right\}$
$(1,3,2)$	$\left\{\begin{matrix} (1,3,2) & (2,3,4) \\ (1,2,4) & (1,4,3) \end{matrix}\right\}$	$\left\{\begin{matrix} (1,3,2) & (1,4,3) \\ (2,3,4) & (1,2,4) \end{matrix}\right\}$

As A_4 has a nontrivial proper normal subgroup K_4, A_4 is not simple.
Quod. Erat. Demonstrandum. ☐

4.4 When $n \geq 5$, A_n Is Simple

Lemma 4.12. When $n \geq 5$, A_n contains all 3-cycles.

Proof. It suffices to notice the following transposition decomposition:

$$(x_1, x_2, x_3) = (x_1, x_3)(x_1, x_2)$$

Quod. Erat. Demonstrandum. ☐

Lemma 4.13. When $n \geq 5$, each $\sigma \in A_n$ is a finite product of 3-cycles.

Proof. It suffices to notice the following three 2-cycle decompositions:

$$(x_1, x_2)(x_3, x_4) = (x_1, x_3, x_2)(x_1, x_3, x_4)$$
$$(x_1, x_2)(x_1, x_3) = (x_1, x_3, x_2)$$
$$(x_1, x_2)(x_1, x_2) = (x_1, x_2, x_3)(x_1, x_2, x_3)$$

Quod. Erat. Demonstrandum. □

Remark: *Three cycles can be viewed as "fundamental building blocks" of A_n.*

Lemma 4.14. Let N be a normal subgroup of A_n, where $n \geq 5$.
If N contains a 3-cycle, then N contains all 3-cycles.

Proof. Assume that N contains a 3-cycle (ξ_1, ξ_2, ξ_3).
Now for all 3-cycle (x_1, x_2, x_3):
Case 1: (x_1, x_2, x_3) and (ξ_1, ξ_2, ξ_3) have 3 common entries.
In this case, $(x_1, x_2, x_3) = (\xi_1, \xi_2, \xi_3) \in N$.
Case 2: (x_1, x_2, x_3) and (ξ_1, ξ_2, ξ_3) have 2 common entries.
In this case, WLOG, assume that $x_1 = \xi_1$ and $x_2 = \xi_2$ and $x_3 \neq \xi_3$,
so choose distinct $x_4, x_5 \in \{x_1, x_2, x_3\}^c$, and define $\sigma = (x_4, x_5)(x_3, \xi_3) \in A_n$,
and we have $(x_1, x_2, x_3) = \sigma(\xi_1, \xi_2, \xi_3)\sigma^{-1} \in N$.
Case 3: (x_1, x_2, x_3) and (ξ_1, ξ_2, ξ_3) have 1 common entry.
In this case, WLOG, assume that $x_1 = \xi_1$ and x_2, x_3, ξ_2, ξ_3 are pairwisely distinct,
so define $\sigma = (x_2, \xi_2)(x_3, \xi_3) \in A_n$, and $(x_1, x_2, x_3) = \sigma(\xi_1, \xi_2, \xi_3)\sigma^{-1} \in N$.
Case 4: (x_1, x_2, x_3) and (ξ_1, ξ_2, ξ_3) have 0 common entry.
In this case, choose distinct $x_4, x_5 \in \{x_1, x_2, x_3\}^c$,
and define $\sigma = (x_1, \xi_1)(x_2, \xi_2)(x_3, \xi_3)(x_4, x_5) \in A_n$,
so $(x_1, x_2, x_3) = \sigma(\xi_1, \xi_2, \xi_3)\sigma^{-1} \in N$.
Hence, A_n contains all 3-cycles. Quod. Erat. Demonstrandum. □

Remark: *For N to be nontrivial and proper, it cannot contain any 3-cycle.*

Lemma 4.15. Let N be a normal subgroup of A_n, where $n \geq 5$.
If N contains an element in the form $\sigma = \mu(x_1, x_2, x_3, \cdots, x_s)$,
where $s \geq 4$ and $\mu, (x_1, x_2, x_3, \cdots, x_s)$ are disjoint,
then N contains a 3-cycle $\sigma^{-1}(x_1, x_2, x_3)\sigma(x_1, x_2, x_3)^{-1} = (x_1, x_3, x_s)$.

Remark: *For N to be nontrivial and proper, the disjoint cycle decomposition of any $\sigma \in N$ cannot contain any s-cycle with $s \geq 4$.*

Lemma 4.16. Let N be a normal subgroup of A_n, where $n \geq 5$.
If N contains an element in the form $\sigma = \mu(x_1, x_2, x_3)(x_4, x_5, x_6)$,
where $\mu, (x_1, x_2, x_3), (x_4, x_5, x_6)$ are pairwise disjoint,
then N contains a 5-cycle $\sigma^{-1}(x_1, x_2, x_4)\sigma(x_1, x_2, x_4)^{-1} = (x_1, x_4, x_2, x_6, x_3)$.

Remark: *For N to be nontrivial and proper, the disjoint cycle decomposition of any $\sigma \in N$ can contain at most one 3-cycle.*

Lemma 4.17. Let N be a normal subgroup of A_n, where $n \geq 5$.
If N contains an element in the form $\sigma = \mu(x_1, x_2)(x_3, x_4)$,
where $r \geq 4$ and $\mu, (x_1, x_2), (x_3, x_4)$ are pairwise disjoint, then:
(1) $\alpha = \sigma^{-1}(x_1, x_2, x_3)\sigma(x_1, x_2, x_3)^{-1} = (x_1, x_3)(x_2, x_4) \in N$.
(2) Take $x_5 \in \{x_1, x_2, x_3, x_4\}^c$. $\beta = (x_1, x_3, x_5) = \beta^{-1}\alpha\beta\alpha \in N$.

Remark: *For N to be nontrivial and proper, the disjoint cycle decomposition of any $\sigma \in N$ can contain at most one 2-cycle.*

Proposition 4.18. When $n \geq 5$, A_n is simple.

Proof. Assume to the contrary that A_n has a nontrivial proper normal subgroup N. There exists a nontrivial element $\sigma \in N$. Previous discussion suggests that the disjoint cycle decomposition of this $\sigma \in N$ must be one of the followings:
Case 1: If $\sigma = (x_1, x_2)$, then $\sigma \notin A_n$, a contradiction.
Case 2: If $\sigma = (x_1, x_2)(x_3, x_4, x_5)$, then $\sigma \notin A_n$, a contradiction.
Hence, our assumption is false, and we've proven that A_n is simple.
Quod. Erat. Demonstrandum. $\square$

References

[1] H. Ren, “Template for math notes,” 2021.

[2] J. Lu and Y. Lau, “Lecture notes: Algebra i,” 2024, hKU, Fall 2024.

[3] 学弱猹, “抽象代数 | 笔记整理（5）——群阶数，西罗定理,” November 2017. [Online]. Available: https://zhuanlan.zhihu.com/p/30845557?utm_psn=1839794425024360448