An application of the First Isomorphism Theorem:

$$\boxed{\text{A group } G \text{ has an index-2 subgroup if and only if there is a surjective homomorphism } G \to \mathbb{Z}_2.}$$

($\Rightarrow$) If $N \leq G$ with $[G:N]=2$, then $N \trianglelefteq G$ (HW 14) and $G/N \cong \mathbb{Z}_2$ since $\mathbb{Z}_2$ is the unique group of order 2, up to isomorphism.

Thus, $\pi: G \to G/N \cong \mathbb{Z}_2$ is a surjective hom.

($\Leftarrow$) If $\varphi: G \to \mathbb{Z}_2$ is surjective, then $\ker\varphi \trianglelefteq G$ and

$$G/\ker\varphi \cong \mathbb{Z}_2,$$

so $[G:\ker\varphi]=2$.

Examples: $A_n \trianglelefteq S_n$

$\langle r \rangle \trianglelefteq D_n$

$\mathbb{R}_{>0} \trianglelefteq \mathbb{R}^\times$

$2\mathbb{Z} \trianglelefteq \mathbb{Z}$

Similarly,

$$\boxed{\text{A group } G \text{ has an index-3 normal subgroup if and only if there is a surjective homomorphism } G \to \mathbb{Z}_3.}$$

An index-3 subgroup is not guaranteed to be normal.

Ex: S_4 has no normal subgroup of order 8.

Why? Suppose $\varphi: S_4 \to \mathbb{Z}_3$ is a homomorphism. Then for all $\sigma \in S_4$, $\varphi(\sigma)$ has order 1 or 3.

But $|\varphi(\sigma)|$ divides $|\sigma|$, so φ must map all even-order elements to 0.

Hence, $\ker \varphi$ contains

- id
- the 6 transpositions
- the 6 4-cycles
- the 3 (2,2)-cycles,

so $|\ker \varphi| > 12$ and $|\ker \varphi|$ divides $|S_4| = 24$ by Lagrange.

Thus, $\ker \varphi = S_4$, so φ is the zero map. In particular, φ is not surjective.

Simple Groups

Def: A group is *simple* if it is not the trivial group, and it has no proper nontrivial subgroups.

i.e. $|G| > 1$ and $N \trianglelefteq G \Rightarrow N = \{e\}$ or $N = G$.

Analogy: $p \in \mathbb{N}$ is prime if $p \neq 1$ and it has no divisors other than 1 and p.

Thm: If G is a simple abelian group, then $G \cong \mathbb{Z}_p$ for a prime p.

Proof: Let G be simple and abelian.

Since $|G| > 1$, there is a non-identity element $g \in G$.

So $\langle g \rangle \neq \{e\}$ is a subgroup, and it is normal since G is abelian.

Thus, $\langle g \rangle = G$. Since we know that

- $|g| = \infty \Rightarrow G \cong \mathbb{Z}$ has infinitely many proper subgroups

and

- $|g| = n \Rightarrow G \cong \mathbb{Z}_n$ has a subgroup for each divisor $d \mid n$,

it must be that $|g| = p$ for a prime p. $\blacksquare$

Thm: A_n is simple for $n \geq 5$

Proof: Book §10.2.

Idea: A nontrivial normal subgroup $N \trianglelefteq A_n$ must contain all 3-cycles. But the 3-cycles generate A_n, so $N = A_n$.

Note: $A_3 \cong \mathbb{Z}_3$ is also simple, but A_4 is not simple (HW 19):

$$H = \{ id, (12)(34), (13)(24), (14)(23) \} \trianglelefteq A_4.$$

Fact: A_5 is the smallest non-abelian simple group $\left(|A_5| = \frac{5!}{2} = 60 \right)$.

The next smallest has order 168.

Thm (Feit-Thompson 1963): If G is a finite non-abelian simple group, then $|G|$ is even.

The proof is 255 pages!

Hölder Program (1870s-1980s)

① Classify all finite simple groups.

② Find all ways to "build" a group out of finite simple groups.

Analogy: ① Find the "primes"

② Understand "prime factorization"

More precisely, ② is the <u>extension problem</u>: Given simple groups A and B, describe all groups G with $N \trianglelefteq G$ such that

- $G/N \cong A$
- $N \cong B$.

Such a G is called an "extension of A by B."

Then: $$\underbrace{\{e\} \trianglelefteq N}_{N/\{e\} \cong B} \trianglelefteq G. \qquad \overbrace{N \trianglelefteq G}^{G/N \cong A}$$

<u>Ex</u>: $A \times B$ is an extension of A by B
(HW 20)

Ex: $A = B = \mathbb{Z}_2$

Two extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2$:

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong V_4$
- $\mathbb{Z}_4$ (with $N = \langle 2 \rangle \cong \mathbb{Z}_2$)

More generally, a <u>composition series</u> for G is a sequence of subgroups $N_0 = \{e\}, N_1, \ldots, N_k = G$ such that

- each $N_i \trianglelefteq N_{i+1}$

  ↳ write $\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = G$

- the quotient groups N_{i+1}/N_i (called the <u>factors</u> of the series) are each simple.

Thm (Jordan-Hölder 1860s-80s):
Let G be a finite group. Then

① G has a composition series; and

② Any two composition series for G have the same length, and the lists of factors are the same (up to reordering and isomorphism).

Analogy: Unique prime factorization.

Def: A group is *solvable* if it has a composition series such that all factors are abelian.

Ex: S_3 is solvable:

$$\overbrace{\{id\} \trianglelefteq A_3}^{A_3 \cong \mathbb{Z}_3} \trianglelefteq S_3 \qquad \underbrace{A_3 \trianglelefteq S_3}_{S_3/A_3 \cong \mathbb{Z}_2}$$

Ex: S_4 is solvable:

$$\overbrace{\{id\} \trianglelefteq \langle (12)(34) \rangle}^{\mathbb{Z}_2} \trianglelefteq H \trianglelefteq A_4 \trianglelefteq S_4 \qquad \underbrace{\langle (12)(34) \rangle \trianglelefteq H}_{\mathbb{Z}_2} \qquad \overbrace{H \trianglelefteq A_4}^{\mathbb{Z}_3} \qquad \underbrace{A_4 \trianglelefteq S_4}_{\mathbb{Z}_2}$$

Ex: S_n is <u>not</u> solvable for $n \geq 5$:

$$\overbrace{\{id\} \trianglelefteq A_n}^{A_n} \trianglelefteq S_n, \qquad \underbrace{A_n \trianglelefteq S_n}_{\mathbb{Z}_2}$$

because A_n is simple and non-abelian.