Ch3 Flashcards

Harley Caham Combest

Fa2025 2025-10-24 MATH5353

Chapter 3 — Quotient Groups and Homomorphisms

Overview. This chapter develops quotient groups from the viewpoint of homomorphisms, establishes normal subgroups as precisely the kernels that make coset-multiplication well-defined, proves Lagrange's Theorem and its consequences, presents the four Isomorphism Theorems, and introduces composition series (Jordan–Hölder) and the alternating groups A_n (including sign and parity). The running theme is that the structure of G is reflected "at the top" by quotients G/N and "at the bottom" by subgroups, with homomorphisms bridging the two.

- **Quotients via homomorphisms.** Fibers of a homomorphism partition G; with the natural "multiply-then-take-fiber" rule these fibers form a group isomorphic to the image. Kernels are subgroups; cosets of the kernel are the elements of the quotient.
- **Normality $\iff$ kernels.** Coset multiplication $uN \cdot vN = (uv)N$ is well-defined iff $gNg^{-1} = N$ for all $g \in G$. Hence $N \lhd G$ iff $N = \ker \varphi$ for some homomorphism, and the natural projection $G \to G/N$ is a homomorphism.
- **Counting.** Lagrange's Theorem: $|H| \mid |G|$ and the number of left cosets is $|G : H|$. Consequences include: orders of elements divide $|G|$; groups of prime order are cyclic.
- **Isomorphism Theorems.** (1) $G/\ker \varphi \cong \operatorname{im} \varphi$; injective $\Leftrightarrow$ trivial kernel. (2) Diamond: if $A \leq N_G(B)$, then $AB/B \cong A/(A \cap B)$. (3) "Invert-and-cancel": $(G/H)/(K/H) \cong G/K$ for $H \lhd K \lhd G$. (4) Lattice: subgroups of G/N correspond bijectively to subgroups of G containing N, preserving inclusions, indices, joins/meets, and normality.
- **Composition series and the Hölder program.** Every finite $G \neq 1$ has a composition series with simple factors; the multiset of factors is unique (Jordan–Hölder). This motivates: classify finite simple groups; then understand extensions that "assemble" them.
- **Alternating group A_n.** Define the sign homomorphism $\varepsilon : S_n \to \{\pm 1\}$ by its action on the Vandermonde product; transpositions have sign -1, so $A_n = \ker \varepsilon$ has order $n!/2$. Parity equals the parity of the number of transpositions in any factorization; a permutation is odd iff it has an odd number of even-length cycles.

3.1 Definitions and Examples.

Fibers and quotients. For a homomorphism $\varphi : G \to H$, fibers over $a \in H$ partition G; multiply fibers by multiplying their images: $X_a \cdot X_b = X_{ab}$. This yields a "quotient group of fibers," naturally isomorphic to $\operatorname{im}\varphi$. Kernels $\ker\varphi = \{g : \varphi(g) = 1\}$ are subgroups; fibers are precisely the left (and right) cosets of the kernel. In $\mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}_n$, the fibers are residue classes $a + n\mathbb{Z}$.

Cosets. For $N \leq G$, $gN = \{gn : n \in N\}$ (left coset), $Ng = \{ng : n \in N\}$ (right coset). The cosets of any subgroup partition G, and $uN = vN \iff v^{-1}u \in N$.

Well-defined multiplication on cosets. The rule $uN \cdot vN = (uv)N$ is well-defined iff $gng^{-1} \in N$ for all $g \in G$, $n \in N$; i.e., iff $N \lhd G$. Equivalently: $gN = Ng$ for all g; or $gNg^{-1} \subseteq N$; or the induced operation on left cosets makes a group G/N. Normality is an embedding property of N in G.

3.2 More on Cosets and Lagrange's Theorem.

Lagrange. For finite G and $H \leq G$, $|G| = |G : H| \cdot |H|$, so $|H| \mid |G|$ and the number of (left/right) cosets is $|G : H|$. Corollaries: the order of any $x \in G$ divides $|G|$, hence $x^{|G|} = 1$; if $|G|$ is prime then G is cyclic. Subgroups of index 2 are normal. The product $HK = \{hk : h \in H, k \in K\}$ has size $|HK| = \frac{|H||K|}{|H \cap K|}$; it is a subgroup iff $HK = KH$ (e.g., if $H \leq N_G(K)$).

3.3 The Isomorphism Theorems.

First. $\ker\varphi \lhd G$ and $G/\ker\varphi \cong \varphi(G)$. Injectivity $\Leftrightarrow \ker\varphi = 1$.

Second (Diamond). If $A \leq N_G(B)$, then AB is a subgroup with $B \lhd AB$ and $AB/B \cong A/(A \cap B)$; indices satisfy $[AB : A] = [B : A \cap B]$.

Third. For $H \lhd K \lhd G$, $(G/H)/(K/H) \cong G/K$ ("invert and cancel").

Fourth (Lattice). Subgroups of G containing $N \lhd G$ correspond bijectively to subgroups of G/N, preserving inclusions, indices, joins/meets, and normality; pictorially, the lattice of G/N appears at the "top" of G's lattice with N collapsed to 1.

3.4 Composition Series and the Hölder Program.

Composition series. A chain $1 = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$ with simple factors N_{i+1}/N_i; existence for finite G and uniqueness of the multiset of factors (Jordan–Hölder). Solvable groups admit chains with abelian (equivalently, cyclic or prime-order) factors; subgroups and quotients of solvable groups are solvable; if N and G/N are solvable, then G is solvable.

Program. (1) Classify finite simple groups (FSCT theorem list); (2) analyze extensions that build general groups from simple factors.

3.5 Transpositions and the Alternating Group.

Generation and parity. Every $\sigma \in S_n$ is a product of transpositions. Define $\varepsilon : S_n \to \{\pm 1\}$ via the Vandermonde product; it is a homomorphism with $\varepsilon((i\,j)) = -1$. Then $A_n = \ker \varepsilon$ has order $n!/2$. The parity of any factorization into transpositions is invariant; a permutation is odd iff the count of even-length cycles in its cycle decomposition is odd.

Small n. $A_1 = A_2 = 1$, $A_3 \cong \mathbb{Z}_3$, $|A_4| = 12$ (isomorphic to the tetrahedron's rotation group; its unique order-4 subgroup is V_4). For $n \geq 5$, A_n is nonabelian simple (proved next chapter).

3.1.1: Exercise 1. Let $\varphi : G \to H$ be a homomorphism and let $E \leq H$. Prove that $\varphi^{-1}(E) \leq G$. If $E \lhd H$, prove that $\varphi^{-1}(E) \lhd G$. Deduce that $\ker \varphi \lhd G$.

As General Proposition: The preimage of a subgroup (resp. normal subgroup) under a group homomorphism is a subgroup (resp. normal subgroup).

As Conditional Proposition: If $\varphi : G \to H$ is a homomorphism and $E \leq H$, then $\varphi^{-1}(E) \leq G$. Moreover, if $E \lhd H$, then $\varphi^{-1}(E) \lhd G$; in particular, $\ker \varphi = \varphi^{-1}(\{1_H\}) \lhd G$.

. . . . . .

Intuition. Homomorphisms respect products and inverses: $\varphi(xy) = \varphi(x)\varphi(y)$ and $\varphi(x^{-1}) = \varphi(x)^{-1}$. So taking preimages "pulls back" the closure properties that define subgroups. Normality is about stability under conjugation; homomorphisms carry conjugation in G to conjugation in H, so normality also pulls back.

. . . . . .

Proof.

Step 1 (Nonemptiness). Since $\varphi(1_G) = 1_H \in E$, we have $1_G \in \varphi^{-1}(E)$, so the preimage is nonempty.

Step 2 (Subgroup test: closure under ab^{-1}). Let $a, b \in \varphi^{-1}(E)$, so $\varphi(a), \varphi(b) \in E$. Because $E \leq H$, $\varphi(a)\varphi(b)^{-1} \in E$. Using homomorphism properties,

$$\varphi(ab^{-1}) = \varphi(a)\,\varphi(b^{-1}) = \varphi(a)\,\varphi(b)^{-1} \in E,$$

hence $ab^{-1} \in \varphi^{-1}(E)$.

Step 3 (Conclude subgroup). By the one-step subgroup criterion (nonempty and closed under ab^{-1}), $\varphi^{-1}(E) \leq G$.

Step 4 (Normality pulls back). Suppose $E \lhd H$. Take any $g \in G$ and any $x \in \varphi^{-1}(E)$. Then $\varphi(x) \in E$, and

$$\varphi(gxg^{-1}) = \varphi(g)\,\varphi(x)\,\varphi(g)^{-1} \in E$$

since E is normal and closed under conjugation in H. Thus $gxg^{-1} \in \varphi^{-1}(E)$, proving $\varphi^{-1}(E) \lhd G$.

Step 5 (Kernel is normal). Take $E = \{1_H\}$, which is normal in H. Then $\ker\varphi = \varphi^{-1}(E) \lhd G$.

3.1.3: Exercise 3. Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

As General Proposition: A quotient of an abelian group is abelian.

As Conditional Proposition: If A is abelian and $B \leq A$, then $B \lhd A$ and the quotient A/B is abelian. Moreover, there exists a non-abelian G with a proper normal $N \lhd G$ such that G/N is abelian (e.g., $G = D_8$, $N = \langle r^2 \rangle$ so that $G/N \cong V_4$).

. . . . . .

Intuition. In an abelian group, every subgroup is automatically normal, so cosets multiply by $(aB)(a'B) = (aa')B$. Since $aa' = a'a$, the coset product commutes, hence the quotient is abelian. For the example, many non-abelian groups become abelian after modding out by a central (or large) normal subgroup; in D_8, collapsing $\langle r^2 \rangle$ kills the "odd" part of the commutator and yields the Klein four-group.

. . . . . .

Proof.

Step 1 (Normality of B). Because A is abelian, $aBa^{-1} = B$ for all $a \in A$; hence $B \lhd A$.

Step 2 (Well-defined multiplication in A/B). For $a_1B, a_2B \in A/B$, define $(a_1B)(a_2B) = (a_1a_2)B$; this is well-defined since $B \lhd A$.

Step 3 (Commutativity in A/B). Using A abelian, $(a_1B)(a_2B) = (a_1a_2)B = (a_2a_1)B = (a_2B)(a_1B)$, so every pair of cosets commutes.

Step 4 (Conclusion for the first part). Therefore A/B is abelian.

. . . . . .

Example (Non-abelian G with abelian G/N).

Step 5 (Pick G and N). Let $G = D_8 = \langle r, s \mid r^4 = s^2 = 1,\ srs = r^{-1} \rangle$, which is non-abelian; take $N = \langle r^2 \rangle = \{1, r^2\}$, a proper normal (indeed central) subgroup.

Step 6 (Compute the quotient). In G/N, we have $(rN)^2 = r^2N = N$ and $(sN)^2 = N$, with rN and sN commuting because $srs = r^{-1}$ implies $sN \cdot rN = r^{-1}N \cdot sN = rN \cdot sN$ in the quotient.

Step 7 (Identify the structure). Thus $G/N = \{N, rN, sN, rsN\}$ with every nontrivial element of order 2 and the operation abelian; hence $G/N \cong V_4$, the Klein four-group.

Step 8 (Conclusion). We have exhibited a non-abelian G and proper normal N with abelian quotient G/N.

3.2.4: Exercise 4. Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$.

As General Proposition: If a finite group has order equal to the product of two primes, then it is either abelian or has trivial center.

As Conditional Proposition: Let G be a finite group with $|G| = pq$ where p, q are primes (possibly $p = q$). Then either G is abelian or $Z(G) = \{1\}$.

. . . . . .

Intuition. If G is not abelian, its center cannot be all of G, so its order must be one of $1, p$, or q by Lagrange. If the center had prime order, then the quotient $G/Z(G)$ would have prime order and hence be cyclic—forcing G itself to be abelian (a standard fact: if $G/Z(G)$ is cyclic then G is abelian). Therefore in the non-abelian case, the only option left is $Z(G) = 1$.

. . . . . .

Proof.

Step 1 (Easy case $p = q$). If $p = q$, then $|G| = p^2$. Every group of order p^2 is abelian (e.g., class equation shows $|Z(G)| > 1$ and then $G/Z(G)$ is cyclic of order p), so the conclusion holds.

Step 2 (Assume G is non-abelian). Suppose G is not abelian. Then $Z(G) \neq G$, hence $Z(G)$ is a proper subgroup. By Lagrange, $|Z(G)| \in \{1, p, q\}$.

Step 3 (Rule out $|Z(G)| = p$ or q). Assume for contradiction $|Z(G)| = p$ (the case $|Z(G)| = q$ is symmetric). Then

$$|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{pq}{p} = q,$$

a prime. Hence $G/Z(G)$ is cyclic.

Step 4 (Lemma: cyclic mod center $\Rightarrow$ abelian). *Claim.* If $G/Z(G)$ is cyclic, then G is abelian. *Proof of claim:* Write $G/Z(G) = \langle gZ(G)\rangle$. For any $x, y \in G$, there exist $a, b \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$ with $x = g^a z_1$, $y = g^b z_2$. Then

$$xy = (g^a z_1)(g^b z_2) = g^{a+b}(z_1 z_2) = g^{a+b}(z_2 z_1) = (g^b z_2)(g^a z_1) = yx,$$

using $z_1, z_2 \in Z(G)$. Hence G is abelian. □

Step 5 (Contradiction). By Step 4, G would be abelian, contradicting Step 2. Therefore our assumption $|Z(G)| = p$ (or q) is impossible.

Step 6 (Conclude the non-abelian case). The only remaining possibility from Step 2 is $|Z(G)| = 1$, i.e., $Z(G) = \{1\}$.

Step 7 (Final dichotomy). Summarizing: either G is abelian (Steps 1 or 4) or, if not, then $Z(G) = 1$ (Step 6). This proves the claim.

3.2.8: Exercise 8. Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

As General Proposition: The intersection of two finite subgroups with relatively prime orders is trivial.

As Conditional Proposition: Let $H, K \leq G$ be finite with $\gcd(|H|, |K|) = 1$. Then $H \cap K = \{1\}$.

. . . . . .

Intuition. The intersection $H \cap K$ is itself a (finite) subgroup of both H and K, so its order must divide *both* $|H|$ and $|K|$ by Lagrange's theorem. If the two orders are relatively prime, the only common divisor is 1, forcing the intersection to be trivial.

. . . . . .

Proof.

Step 1 (Intersection is a subgroup). Since intersections of subgroups are subgroups, $H \cap K \leq H$ and $H \cap K \leq K$.

Step 2 (Apply Lagrange to each containment). By Lagrange's theorem, $|H \cap K| \mid |H|$ and also $|H \cap K| \mid |K|$.

Step 3 (Use relative primeness). Because $\gcd(|H|, |K|) = 1$, the only positive integer dividing both $|H|$ and $|K|$ is 1. Hence $|H \cap K| = 1$.

Step 4 (Conclude). Therefore $H \cap K$ is the trivial subgroup: $H \cap K = \{1\}$.

3.2.11: Exercise 11. Let $H \leq K \leq G$. Prove that $[G : H] = [G : K] \cdot [K : H]$ (do not assume G is finite).

As General Proposition: For subgroups $H \leq K \leq G$, the index is multiplicative: $[G : H] = [G : K]\,[K : H]$, interpreting any side as ∞ when the corresponding index is infinite.

As Conditional Proposition: If $H \leq K \leq G$ and both $[G : K]$ and $[K : H]$ are finite, then $[G : H] = [G : K] \cdot [K : H]$. If either $[G : K] = \infty$ or $[K : H] = \infty$, then $[G : H] = \infty$.

. . . . . .

Intuition. Cosets of H sit inside cosets of K. Pick representatives $g_1, \ldots, g_m$ for the K-cosets in G and $h_1, \ldots, h_n$ for the H-cosets in K. Then every element of G lands in exactly one of the mn subsets $g_i h_j H$, which are distinct left cosets of H. Thus mn is the number of H-cosets. If one of the indices is infinite, containment of cosets forces $[G : H]$ to be infinite as well.

. . . . . .

Proof.

Step 1 (Reduce infinite cases to triviality). If $[G : K] = \infty$, then there are infinitely many distinct K-cosets in G, each containing at least one H-coset, hence $[G : H] = \infty$. If $[K : H] = \infty$, then K already has infinitely many H-cosets, so G has at least that many; thus $[G : H] = \infty$. Hence it suffices to treat the case where $m = [G : K] < \infty$ and $n = [K : H] < \infty$.

Step 2 (Choose representatives). Fix representatives $g_1, \ldots, g_m$ of the distinct left cosets of K in G so that $G = \bigsqcup_{i=1}^{m} g_i K$. Fix representatives $h_1, \ldots, h_n$ of the distinct left cosets of H in K so that $K = \bigsqcup_{j=1}^{n} h_j H$.

Step 3 (Cover G by mn H-cosets). For any $g \in G$ there exists a unique i with $g \in g_i K$; write $g = g_i k$ for some $k \in K$. Then $k \in h_j H$ for a unique j, so $k = h_j h$ with $h \in H$, hence $g = g_i h_j h \in g_i h_j H$. Therefore

$$G = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} g_i h_j H.$$

Step 4 (Distinctness of the mn cosets). Suppose $g_i h_j H = g_{i'} h_{j'} H$. Then $g_i^{-1} g_{i'} \in h_j H h_{j'}^{-1} \subseteq K$; hence $g_i K = g_{i'} K$, forcing $i = i'$. With $i = i'$, we have $h_j H = h_{j'} H$ inside K, hence $j = j'$. Thus the mn cosets $g_i h_j H$ are pairwise distinct.

Step 5 (Count and conclude). By Steps 3–4, the distinct left cosets of H in G are exactly the mn sets $\{\, g_i h_j H \,\}$, so $[G : H] = mn = [G : K] \cdot [K : H]$. This also matches the infinite cases from Step 1, completing the proof.

3.3.7: Exercise 7. Let M and N be normal subgroups of G such that $G = MN$. Prove that

$$G/(M \cap N) \;\cong\; (G/M) \times (G/N).$$

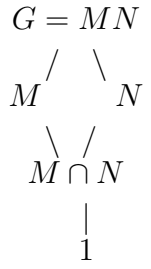
[Draw the lattice.]

As General Proposition: If $M, N \lhd G$ and $G = MN$, then the natural map $G \to (G/M)\times(G/N)$ is surjective with kernel $M\cap N$, hence $G/(M\cap N) \cong (G/M)\times(G/N)$.

As Conditional Proposition: Under the same hypotheses, the isomorphism is induced by $g \mapsto (gM, gN)$.

. . . . . .

Lattice picture.



(Lines in the "top diamond" correspond to quotienting by $M \cap N$.)

. . . . . .

Intuition. The map $\varphi(g) = (gM, gN)$ records g modulo each normal subgroup. Elements indistinguishable mod *both* M and N differ by an element of $M \cap N$, so $\ker\varphi = M \cap N$. The hypothesis $G = MN$ lets us hit any pair of cosets (xM, yN) by multiplying a suitable element from N (to set the G/M-coordinate) with one from M (to set the G/N-coordinate), so φ is onto. First Isomorphism Theorem finishes.

. . . . . .

Proof.

Step 1 (Define the map). Define $\varphi : G \to (G/M) \times (G/N)$ by $\varphi(g) = (gM, gN)$. Since $M, N \lhd G$, the quotients are groups and φ is a homomorphism:

$$\varphi(ab) = \big(abM, abN\big) = \big(aM, bM\big)\big(bN, bN\big) = \varphi(a)\varphi(b).$$

Step 2 (Kernel). If $g \in \ker\varphi$ then $gM = M$ and $gN = N$, i.e., $g \in M \cap N$. Conversely, any $g \in M \cap N$ maps to (M, N), so $\ker\varphi = M \cap N$.

Step 3 (Image contains the "axes").

(a) Points of the form (xM, N). Let $xM \in G/M$. Since $G = MN$, choose $x = mn$ with $m \in M$, $n \in N$. Then $xM = nM$, so

$$(xM, N) = (nM, N) = \varphi(n) \in \operatorname{im}\varphi.$$

(b) Points of the form (M, yN). Let $yN \in G/N$. Again write $y = mn$ with $m \in M$, $n \in N$. Then $yN = mN$, so

$$(M, yN) = (M, mN) = \varphi(m) \in \operatorname{im}\varphi.$$

Step 4 (Surjectivity). The image $\operatorname{im}\varphi$ is a subgroup of $(G/M)\times(G/N)$ containing all (xM, N) and all (M, yN) by Step 3; hence it contains their products $(xM, N) \cdot$

$(M, yN) = (xM, yN)$. Therefore φ is surjective.

Step 5 (Apply First Isomorphism Theorem). With $\ker \varphi = M \cap N$ (Step 2) and φ onto (Step 4), the First Isomorphism Theorem gives

$$G/(M \cap N) \;\cong\; (G/M) \times (G/N).$$

Step 6 (Conclusion). The desired isomorphism is realized by $g(M \cap N) \longmapsto (gM, gN)$.

3.3.10: Exercise 10. Generalize the preceding exercise as follows. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $\gcd\big([G:H],\,|H|\big)=1$. Prove that if H is a Hall subgroup of G and $N \lhd G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.

As General Proposition: If G is finite, $H \leq G$ is Hall, and $N \lhd G$, then

$$\gcd\big([N:H\cap N],\,|H\cap N|\big)=1 \quad \text{and} \quad \gcd\big([G/N:HN/N],\,|HN/N|\big)=1.$$

Equivalently, $H \cap N$ is Hall in N and HN/N is Hall in G/N.

As Conditional Proposition: Let G be finite, $H \leq G$ with $\gcd([G:H],|H|)=1$, and let $N \lhd G$. Then $H \cap N$ is Hall in N, and HN/N is Hall in G/N.

. . . . . .

Intuition. Intersections and products behave well with indices:

$$[N : H \cap N] = [HN : H] \quad \text{and} \quad [G/N : HN/N] = [G : HN].$$

Both numbers divide $[G : H]$ via $[G : H] = [G : HN]\,[HN : H]$. Thus any prime dividing those indices cannot divide $|H|$. Since $|H \cap N| \mid |H|$ and $|HN/N| \mid |H|$, the relative primeness descends to $H \cap N$ and to HN/N.

. . . . . .

Proof.

Step 1 (Index factorizations). Because $H \leq HN \leq G$, we have

$$[G : H] = [G : HN]\,[HN : H]. \tag{$*$}$$

Also, for any $N \leq G$, the standard index formula gives

$$[N : H \cap N] = [HN : H]. \tag{$\dagger$}$$

Finally, since $N \lhd G$, the natural projection $G \to G/N$ yields

$$[G/N : HN/N] = [G : HN]. \tag{$\ddagger$}$$

Step 2 (Divisibility into the Hall index). From $(*)$ and $(\dagger)$ we see that

$$[N : H \cap N] = [HN : H] \;\mid\; [G : H].$$

From $(*)$ and $(\ddagger)$ we see that

$$[G/N : HN/N] = [G : HN] \;\mid\; [G : H].$$

Step 3 (Orders divide $|H|$). By Lagrange, $|H \cap N| \mid |H|$. Also,

$$|HN/N| = \frac{|HN|}{|N|} = \frac{|H||N|/|H \cap N|}{|N|} = \frac{|H|}{|H \cap N|} \;\mid\; |H|.$$

Step 4 (Coprimeness for the intersection). Since H is Hall in G, $\gcd([G : H], |H|) = 1$. Using Step 2 and Step 3,

$$[N : H \cap N] \mid [G : H] \quad \text{and} \quad |H \cap N| \mid |H| \;\Rightarrow\; \gcd\big([N : H \cap N],\, |H \cap N|\big) = 1.$$

Thus $H \cap N$ is a Hall subgroup of N.

Step 5 (Coprimeness for the quotient). Again by Steps 2–3,

$$[G/N : HN/N] \mid [G : H] \quad \text{and} \quad |HN/N| \mid |H| \;\Rightarrow\; \gcd\big([G/N : HN/N],\, |HN/N|\big) = 1.$$

Hence HN/N is a Hall subgroup of G/N.

Step 6 (Conclusion). Both claims follow: intersections with N preserve the Hall property inside N, and passing to G/N sends H to the Hall subgroup HN/N.

3.4.6: Exercise 6. Prove part (1) of the Jordan–Hölder Theorem by induction on $|G|$.

As General Proposition: Every finite nontrivial group G has a composition series.

As Conditional Proposition: If G is a finite group with $|G| \geq 2$, then there exist normal subgroups

$$1 \;=\; G_0 \lhd G_1 \lhd \cdots \lhd G_k \;=\; G$$

such that each factor G_{i+1}/G_i is simple.

. . . . . .

Intuition. Build the series from the bottom up. If G is simple, we are done: $1 \lhd G$. Otherwise pick a largest proper normal subgroup $N \lhd G$. By induction, N already has a composition series. Maximality of N forces G/N to be simple; appending $N \lhd G$ on top of a composition series of N yields one for G.

. . . . . .

Proof (by induction on $|G|$).

Step 1 (Base case). If $|G| = 1$ the statement is vacuous; if $|G|$ is prime (or G is simple), then $1 \lhd G$ is a composition series, since $G/1 \cong G$ is simple.

Step 2 (Inductive hypothesis). Assume every nontrivial group of order $< |G|$ has a composition series. Suppose G is a finite group with $|G| \geq 2$.

Step 3 (If G is simple, done). If G is simple, we again have the series $1 \lhd G$ and are finished. So assume G is not simple.

Step 4 (Choose a maximal proper normal subgroup). Because G is not simple, there exists $1 \neq N \lhd G$ with $N \neq G$. Choose N maximal among proper normal subgroups of G (by finiteness such a choice exists).

Step 5 (Apply induction to N). Since $1 < |N| < |G|$, the inductive hypothesis gives a composition series

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_r = N$$

with each G_{i+1}/G_i simple.

Step 6 (Show G/N is simple). Suppose G/N is not simple. Then there exists a normal subgroup $\overline{M} \trianglelefteq G/N$ with $1 \neq \overline{M} \neq G/N$. Let M be the full preimage of $\overline{M}$ in G. Then $N < M < G$ and $M \trianglelefteq G$ (preimage of a normal subgroup under the projection $G \to G/N$). This contradicts the maximality of N. Hence G/N is simple.

Step 7 (Assemble the series for G). Appending $N \lhd G$ to the series for N produces

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_r = N \lhd G,$$

whose factors are the simple groups G_{i+1}/G_i for $0 \leq i < r$ and G/N on top. Thus all successive quotients are simple, so this is a composition series for G.

Step 8 (Conclusion). By induction on $|G|$, every finite nontrivial group has a composition series.

3.4.9: Exercise 9. Prove the following special case of part (2) of the Jordan–Hölder Theorem: assume the finite group G has two composition series

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_r = G \qquad \text{and} \qquad 1 = M_0 \lhd M_1 \lhd M_2 = G.$$

Show that $r = 2$ and that the list of composition factors is the same. *[Use the Second Isomorphism Theorem.]*

As General Proposition: If G has a composition series of length 2, then every composition series of G also has length 2, and its two factors are (up to order) M_1 and G/M_1.

As Conditional Proposition: Under the hypotheses above, necessarily $r = 2$ and

$$N_1 \;\cong\; M_1, \qquad G/N_1 \;\cong\; G/M_1.$$

Thus the two composition factors coincide (up to permutation).

. . . . . .

Intuition. Because $M_1 \lhd G$ and G/M_1 is simple, every subgroup $X \leq G$ either lies in M_1 or, together with M_1, generates all of G. Apply this dichotomy to the terms of the other series. Locate the last N_i still inside M_1. The next term N_{i+1} must "jump over" M_1 so that $N_{i+1}M_1 = G$. The Second Isomorphism Theorem then gives

$$N_{i+1}/(N_{i+1} \cap M_1) \;\cong\; (N_{i+1}M_1)/M_1 \cong G/M_1,$$

so $N_{i+1} \cap M_1$ is trivial because M_1 is simple. This forces $i = 0$ and shows N_1 is simple and intersects M_1 trivially, while $N_1M_1 = G$. A second use of the theorem yields $G/N_1 \cong M_1$, hence there is no room for further terms: $r = 2$.

. . . . . .

Proof.

Step 1 (Simple building blocks). Since $1 \lhd M_1 \lhd G$ is a composition series, M_1 and G/M_1 are simple, with $M_1 \lhd G$.

Step 2 (Dichotomy for the N_i's). For any $X \leq G$, the subgroup $(XM_1)/M_1$ is a (normal) subgroup of G/M_1; because G/M_1 is simple, either $XM_1 = M_1$ (hence $X \leq M_1$) or $XM_1 = G$. Apply this to each N_i.

Step 3 (Locate the jump index). Let i be maximal with $N_i \leq M_1$. Then $N_{i+1} \not\leq M_1$, so by Step 2 we have $N_{i+1}M_1 = G$.

Step 4 (First use of Second Isomorphism). The Second Isomorphism Theorem gives

$$(N_{i+1}M_1)/M_1 \;\cong\; N_{i+1}/(N_{i+1} \cap M_1).$$

Since $N_{i+1}M_1 = G$, the left side is G/M_1, which is simple. Hence $N_{i+1}/(N_{i+1} \cap M_1)$ is simple.

Step 5 (Intersect with M_1). Consider $M_1/(M_1 \cap N_{i+1})$. By the same theorem,

$$(M_1N_{i+1})/N_{i+1} \;\cong\; M_1/(M_1 \cap N_{i+1}).$$

Here $M_1N_{i+1} = G$, so the left side is G/N_{i+1}. Thus $M_1/(M_1 \cap N_{i+1}) \cong G/N_{i+1}$. Because M_1 is simple, $M_1 \cap N_{i+1}$ is either 1 or M_1. It cannot be M_1 (else $N_{i+1} \leq M_1$, contradicting Step 3), so $M_1 \cap N_{i+1} = 1$.

Step 6 (Identify the lower factor and force $i = 0$). From Step 4 and $N_{i+1} \cap M_1 = 1$, we get $N_{i+1} \cong G/M_1$, hence N_{i+1} is simple. Since $N_i \leq M_1$ and $N_i \lhd N_{i+1}$ (composition chain), the only possibility—because $M_1 \cap N_{i+1} = 1$—is $N_i = 1$. Therefore $i = 0$ and N_1 is simple.

Step 7 (Identify the upper factor and rule out intermediates). Using Step

5 with $M_1 \cap N_1 = 1$ gives $G/N_1 \cong M_1$, which is simple. Hence there is no proper subgroup strictly between N_1 and G; therefore the N-series must be

$$1 = N_0 \lhd N_1 \lhd N_2 = G,$$

so $r = 2$.

Step 8 (Match the factors). The two composition factors for the N-series are $N_1/1 \cong N_1$ and $G/N_1 \cong M_1$. Since $N_1 \cong G/M_1$ (Step 6), the multiset $\{ N_1, G/N_1 \}$ equals $\{ M_1, G/M_1 \}$ up to order. Thus both series have the same two factors.

Step 9 (Conclusion). Any composition series of G has length 2, and its factors are precisely M_1 and G/M_1 (up to permutation), as required.

3.5.4: Exercise 4. Show that $S_n = \langle (1\ 2),\ (1\ 2\ \cdots\ n) \rangle$ for all $n \geq 2$.

As General Proposition: The symmetric group S_n is generated by a single transposition and an n-cycle.

As Conditional Proposition: For $n \geq 2$, letting $\tau = (1\ 2)$ and $\sigma = (1\ 2\ \cdots\ n)$, we have $S_n = \langle \tau, \sigma \rangle$.

. . . . . .

Intuition. Conjugating a transposition by a cycle "shifts" its entries. Thus the conjugates $\sigma^i \tau \sigma^{-i}$ produce all adjacent transpositions $(i+1\ i+2)$ (indices read in $\{1, \ldots, n\}$). Since adjacent transpositions generate S_n, the pair $\{\tau, \sigma\}$ already generates S_n.

. . . . . .

Proof.

Step 1 (Conjugation shift). For $0 \le i \le n-2$,

$$\sigma^{\,i}\,\tau\,\sigma^{-i} \;=\; \sigma^{\,i}\,(1\ 2)\,\sigma^{-i} \;=\; (1+i,\ 2+i),$$

where we interpret $k+i$ modulo n but keep representatives in $\{1, \ldots, n\}$. Hence

$$(1\ 2),\ (2\ 3),\ \ldots,\ (n-1\ n) \;\in\; \langle \tau, \sigma \rangle.$$

Step 2 (Adjacent transpositions generate S_n). It is standard that $S_n = \langle (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle$ (every transposition, hence every permutation, is a product of adjacent swaps).

Step 3 (Conclusion). Since all adjacent transpositions lie in $\langle \tau, \sigma \rangle$, we have

$$S_n = \langle (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle \;\subseteq\; \langle \tau, \sigma \rangle \;\subseteq\; S_n,$$

giving equality $S_n = \langle \tau, \sigma \rangle$.

3.5.12: Exercise 12. Prove that A_n contains a subgroup isomorphic to S_{n-2} for each $n \geq 3$.

As General Proposition: For $n \geq 3$, there is an injective homomorphism $S_{n-2} \hookrightarrow A_n$; hence A_n has a subgroup isomorphic to S_{n-2}.

As Conditional Proposition: Fix $n \geq 3$ and write $\Omega = \{1, \ldots, n-2\}$. Define $\Phi : S_{n-2} \to A_n$ by

$$\Phi(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \text{ is even (acting trivially on } n-1, n); \\ \sigma \circ (n-1\ n), & \text{if } \sigma \text{ is odd.} \end{cases}$$

Then Φ is an injective homomorphism, so $\Phi(S_{n-2}) \leq A_n$ and $\Phi(S_{n-2}) \cong S_{n-2}$.

. . . . . .

Intuition. Let S_{n-2} permute $\{1, \dots, n-2\}$ and leave $\{n-1, n\}$ fixed; those with even sign already lie in A_n. Odd ones can be "corrected" by multiplying by the transposition $(n-1\ n)$, which flips the sign without disturbing the action on $\{1, \dots, n-2\}$. This parity-fixing trick embeds S_{n-2} into A_n.

. . . . . .

Proof.

Step 1 (Well-defined target lies in A_n). If $\sigma \in S_{n-2}$ is even, then $\Phi(\sigma) = \sigma$ fixes $n-1, n$ and has even sign, hence $\Phi(\sigma) \in A_n$; if σ is odd, then $\Phi(\sigma) = \sigma(n-1\ n)$ has sign $(-1) \cdot (-1) = +1$, so $\Phi(\sigma) \in A_n$.

Step 2 (Homomorphism property). Let $\sigma, \tau \in S_{n-2}$ and write $\varepsilon(\cdot) \in \{\pm 1\}$ for the sign on S_n. Then

$$\Phi(\sigma) = \sigma\,(n-1\ n)^{\frac{1-\varepsilon(\sigma)}{2}}, \qquad \Phi(\tau) = \tau\,(n-1\ n)^{\frac{1-\varepsilon(\tau)}{2}}.$$

Since $(n-1\ n)$ commutes with every permutation of Ω, we have

$$\Phi(\sigma)\Phi(\tau) = \sigma\tau\,(n-1\ n)^{\frac{1-\varepsilon(\sigma)}{2}+\frac{1-\varepsilon(\tau)}{2}} = \sigma\tau\,(n-1\ n)^{\frac{1-\varepsilon(\sigma)\varepsilon(\tau)}{2}} = \Phi(\sigma\tau),$$

establishing that Φ is a homomorphism.

Step 3 (Injectivity). Suppose $\Phi(\sigma) = \Phi(\tau)$. Restrict both sides to Ω; $(n-1\ n)$ acts trivially on Ω, so the restriction equals σ on the left and τ on the right, yielding $\sigma = \tau$. Hence $\ker \Phi = \{1\}$ and Φ is injective.

Step 4 (Conclusion). The image $\Phi(S_{n-2})$ is a subgroup of A_n isomorphic to S_{n-2} by injectivity; therefore A_n contains a subgroup isomorphic to S_{n-2}.