Ch2 Flashcards

Harley Caham Combest

Fa2025 2025-10-24 MATH5353

. . . .

Chapter 2 — Subgroups

. . . .

This chapter develops the language and core tools for working with *subgroups*: quick tests to recognize them, large natural families (centralizers, normalizers, stabilizers, kernels), a full treatment of cyclic groups and their subgroups, how arbitrary subsets generate subgroups, and how to visualize inclusion relations via the lattice of subgroups.

- **Recognizing subgroups fast.** The *Subgroup Criterion* replaces "check all axioms" with a two-line test: $H \neq \varnothing$ and $xy^{-1} \in H$ for all $x, y \in H$ (and for finite H, nonempty + closure under multiplication suffices).
- **Natural subgroups from actions.** Centralizers $C_G(A)$, normalizers $N_G(A)$, the center $Z(G)$, stabilizers G_s, and kernels of actions are all subgroups; they organize commutation and symmetry-by-conjugation.
- **Cyclic structure in full.** A cyclic group $\langle x \rangle$ has $|\langle x \rangle| = |x|$. Any two cyclic groups of the same order are isomorphic; orders of powers and the precise list of generators are determined by gcd relations.
- **Generating by subsets.** For $A \subseteq G$, the subgroup $\langle A \rangle$ is the *intersection of all subgroups* containing A, equivalently the set of all finite words in $A^{\pm 1}$.
- **Lattice viewpoint.** The subgroup lattice encodes joins ($\langle H, K \rangle$) and intersections graphically; partial lattices focus on just the relationships of interest.

2.1 Definition and Examples

Definition. A subset $H \subseteq G$ is a *subgroup* (written $H \leq G$) if $H \neq \varnothing$ and H is closed under taking inverses and products (equivalently, $x, y \in H \Rightarrow xy^{-1} \in H$).

Subgroup Criterion. $H \leq G$ iff $H \neq \varnothing$ and $xy^{-1} \in H$ for all $x, y \in H$. If H is finite, it suffices to check $H \neq \varnothing$ and closure under multiplication.

Basic consequences.

- The identity of H equals the identity of G; inverses coincide as elements of G.
- Transitivity: if $K \leq H \leq G$, then $K \leq G$.
- Many yes/no examples illustrate pitfalls: wrong operation, missing identity, not inverse-closed.

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Centralizer/Center. $C_G(A) = \{g \in G \mid ga = ag \ \forall a \in A\}$ and $Z(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ are subgroups. Always $Z(G) = C_G(G)$.

Normalizer. $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$ is a subgroup and contains $C_G(A)$. Conjugation on subsets explains both as stabilizer/kernel of an action.

Actions $\Rightarrow$ subgroups. For a G-action on S, the stabilizer $G_s = \{g \mid g \cdot s = s\}$ and the kernel $\{g \mid g \cdot t = t \ \forall t \in S\}$ are subgroups. Many concrete computations (e.g., in D_8, S_3) follow quickly from these definitions.

2.3 Cyclic Groups and Cyclic Subgroups

Cyclic. $\langle x\rangle = \{x^n \mid n \in \mathbb{Z}\}$ is abelian. If $|\langle x\rangle| = n < \infty$, then the distinct elements are $1, x, \ldots, x^{n-1}$; if $|\langle x\rangle| = \infty$, all powers are distinct.

Divisibility of orders. If $x^m = 1$ and $x^n = 1$, then $x^{\gcd(m,n)} = 1$; in particular $|x| \mid m$ whenever $x^m = 1$.

All cyclics look alike. Any two cyclic groups of the same order are isomorphic; infinite cyclic $\cong \mathbb{Z}$, finite cyclic of order $n \cong \mathbb{Z}/n\mathbb{Z}$.

Orders of powers. If $|x| = \infty$, then $|x^a| = \infty$ for $a \neq 0$. If $|x| = n < \infty$, then $|x^a| = \dfrac{n}{\gcd(n,a)}$.

Generators. In $\langle x\rangle$ with $|x| = n$, the element x^a generates the whole group iff $\gcd(a,n) = 1$; hence the number of generators is $\varphi(n)$.

Subgroups of cyclic groups (complete classification).

- Every subgroup of a cyclic group is cyclic.
- If $|\langle x\rangle| = \infty$, its nontrivial subgroups are exactly $\langle x^m\rangle$ for $m \in \mathbb{Z}_{>0}$, all distinct.
- If $|\langle x\rangle| = n$, then for each $a \mid n$ there is a unique subgroup of order a, namely $\langle x^{n/a}\rangle$.

2.4 Subgroups Generated by Subsets of a Group

Definition. For $A \subseteq G$, the subgroup *generated by* A is

$$\langle A \rangle = \bigcap \{H \leq G \mid A \subseteq H\},$$

the unique smallest subgroup containing A.

Word description. Equivalently,

$$\langle A \rangle = \{a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \mid n \geq 0,\ a_i \in A,\ \varepsilon_i \in \{\pm 1\}\},$$

i.e., all finite products of elements of A and their inverses. In abelian G with $A = \{a_1, \ldots, a_k\}$,

$$\langle A \rangle = \{a_1^{m_1} \cdots a_k^{m_k} \mid m_i \in \mathbb{Z}\}.$$

Intersections are subgroups. Arbitrary intersections of (nonempty families of) subgroups are subgroups; this underpins the "smallest subgroup containing A."

2.5 The Lattice of Subgroups of a Group

Lattice picture. Plot all subgroups from 1 (bottom) to G (top), connecting H upward to K when $H < K$ with no subgroup strictly between. The diagram reveals:

- *Join* $\langle H, K\rangle$ by tracing upward until a first common subgroup is reached.
- *Meet* $H \cap K$ by tracing downward to the largest subgroup contained in both.

Usage. Even partial lattices (for finite or infinite groups) help read off joins, intersections, and often simplify centralizer/normalizer computations (e.g., in D_{2n}, Q_8, S_3).

2.1: Exercise 1(c). For fixed $n \in \mathbb{Z}_{>0}$, prove that the set of rational numbers whose denominators divide n (under addition) is a subgroup of $(\mathbb{Q}, +)$.

As General Proposition: For any $n \in \mathbb{Z}_{>0}$, the subset

$$H_n = \left\{ \tfrac{a}{b} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z},\ b \in \mathbb{Z}_{>0},\ \gcd(a, b) = 1,\ b \mid n \right\}$$

is a subgroup of $(\mathbb{Q}, +)$.

As Conditional Proposition: Fix $n \in \mathbb{Z}_{>0}$. Then $H_n \leq (\mathbb{Q}, +)$.

. . . .

Intuition. Use the subgroup criterion for additive groups: a nonempty subset H is a subgroup iff it is closed under subtraction. If two rationals have denominators dividing the same n, then after putting them over the common denominator n, their difference again has (reduced) denominator dividing n.

. . . .

Proof.
Step 1 (Define the candidate set). Let $H := H_n = \{\frac{a}{b} \in \mathbb{Q} \mid \gcd(a,b) = 1,\ b \mid n\}$.
Step 2 (Nonemptiness). $0 = \frac{0}{1} \in H$ since $1 \mid n$; hence $H \neq \varnothing$.
Step 3 (Closure under subtraction). Take $\frac{a}{b}, \frac{c}{d} \in H$ in lowest terms, so $b \mid n$ and $d \mid n$. Write $n = bx = dy$ for some $x, y \in \mathbb{Z}_{>0}$. Then

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} = \frac{ax - cy}{n}.$$

Reduce $\frac{ax-cy}{n}$ to lowest terms: say $\frac{ax-cy}{n} = \frac{p}{q}$ with $\gcd(p,q) = 1$. Since q is a (positive) divisor of n, we have $q \mid n$, hence $\frac{p}{q} \in H$. Thus H is closed under subtraction.
Step 4 (Conclude by subgroup criterion). By Steps 2–3 and the subgroup criterion ($H \neq \varnothing$ and closed under subtraction $\Rightarrow H \leq \mathbb{Q}$), we conclude $H \leq (\mathbb{Q}, +)$.

2.1: Exercise 3(a). In the dihedral group $D_8 = \langle r, s \mid r^4 = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$, show that $\{1, r^2, s, sr^2\}$ is a subgroup.

As General Proposition: In D_8, the set $H := \{1, r^2, s, sr^2\}$ is a subgroup (indeed, a Klein 4-group).

As Conditional Proposition: Let $D_8 = \langle r, s \mid r^4 = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$. Then $H = \{1, r^2, s, sr^2\} \leq D_8$.

. . . .

Intuition. Because D_8 is finite, it suffices to check closure under the group operation. Use the relations $r^4 = 1$, $s^2 = 1$, and $r^k s = sr^{-k}$ (equivalently $sr^k = r^{-k}s$) to multiply any two listed elements and verify the product lands back in H.

. . . .

Proof.

Step 1 (Nonempty). $1 \in H$, so $H \neq \varnothing$.

Step 2 (Useful identities). From $srs = r^{-1}$ we have $r^k s = sr^{-k}$ and $sr^k = r^{-k}s$ for all $k \in \mathbb{Z}$; also $r^4 = 1$ and $s^2 = 1$.

Step 3 (Squares). $r^2 \cdot r^2 = 1 \in H$, $s \cdot s = 1 \in H$, and $(sr^2) \cdot (sr^2) = sr^2sr^2 = (sr^2s)r^2 = r^{-2}r^2 = 1 \in H$.

Step 4 (Mixed products with r^2). $r^2 \cdot s = r^2 s = sr^{-2} = sr^2 \in H$ and $r^2 \cdot (sr^2) = r^2sr^2 = (sr^2)r^2 = sr^4 = s \in H$.

Step 5 (Mixed products with s). $s \cdot r^2 = sr^2 \in H$ and $s \cdot (sr^2) = (ss)r^2 = r^2 \in H$.

Step 6 (Mixed products with sr^2). $(sr^2) \cdot r^2 = sr^2r^2 = sr^4 = s \in H$ and $(sr^2) \cdot s = sr^2s = r^{-2} = r^2 \in H$.

Step 7 (Closure and subgroup). All products of elements of H remain in H; since D_8 is finite, closure implies inverses exist in H; hence $H \leq D_8$.

2.1: Exercise 3(b). In the dihedral group D_8, show that $\{1, r^2, sr, sr^3\}$ is a subgroup.

As General Proposition: In D_8, the set $K := \{1, r^2, sr, sr^3\}$ is a subgroup (also a Klein 4-group).

As Conditional Proposition: With $D_8 = \langle r, s \mid r^4 = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$, we have $K = \{1, r^2, sr, sr^3\} \leq D_8$.

. . . .

Intuition. Again use finiteness and the relations to enumerate products. The reflections sr and sr^3 both square to 1, and multiplying by r^2 toggles them, keeping us inside K.

. . . .

Proof.

Step 1 (Nonempty). $1 \in K$, so $K \neq \varnothing$.
Step 2 (Squares). $r^2 \cdot r^2 = 1$; $(sr)\cdot(sr) = srsr = (srs)r = r^{-1}r = 1$; $(sr^3)\cdot(sr^3) = sr^3sr^3 = (sr^3s)r^3 = r^{-3}r^3 = 1$.
Step 3 (Products with r^2). $r^2 \cdot (sr) = (r^2s)r = (sr^2)r = sr^3 \in K$ and $r^2 \cdot (sr^3) = (r^2s)r^3 = (sr^2)r^3 = sr^5 = sr \in K$.
Step 4 (Reverse products with r^2). $(sr) \cdot r^2 = sr^2 \cdot r = (sr^2)r = sr^3 \in K$ and $(sr^3) \cdot r^2 = sr^3r^2 = sr^5 = sr \in K$.
Step 5 (Cross products of reflections). $(sr)\cdot(sr^3) = srsr^3 = (srs)r^3 = r^{-1}r^3 = r^2 \in K$ and $(sr^3) \cdot (sr) = sr^3sr = (sr^3s)r = r^{-3}r = r^2 \in K$.
Step 6 (Closure and subgroup). Every product of elements of K lies in K; by finiteness, inverses lie in K as well; thus $K \leq D_8$.

2.2: Exercise 2. Prove that $C_G\big(Z(G)\big) = G$ and deduce that $N_G\big(Z(G)\big) = G$.

As General Proposition: For any group G, its center $Z(G)$ satisfies

$$C_G\big(Z(G)\big) = G \qquad \text{and} \qquad N_G\big(Z(G)\big) = G.$$

As Conditional Proposition: Let G be a group. Then every $g \in G$ centralizes and normalizes $Z(G)$; hence $C_G(Z(G)) = N_G(Z(G)) = G$.

. . . .

Intuition. Elements of $Z(G)$ commute with *everything*. So conjugating any $z \in Z(G)$ by any $g \in G$ leaves z unchanged. That means every g centralizes the whole center, and in particular stabilizes it under conjugation, so both the centralizer and normalizer are all of G.

. . . .

Proof.

Step 1 (Center definition). $Z(G) = \{z \in G \mid \forall x \in G,\ zx = xz\}$.

Step 2 ($G \subseteq C_G(Z(G))$). Fix arbitrary $g \in G$ and $z \in Z(G)$. Since z commutes with every element of G, in particular with g, we have $gz = zg$, hence $gzg^{-1} = z$. Thus g commutes with every element of $Z(G)$, i.e. $g \in C_G(Z(G))$. Because g was arbitrary, $G \subseteq C_G(Z(G))$.

Step 3 (Equality). Trivially $C_G(Z(G)) \subseteq G$, so $C_G(Z(G)) = G$.

Step 4 (Normalizer). For any subset $A \subseteq G$, $C_G(A) \leq N_G(A)$. Applying this with $A = Z(G)$ gives

$$G = C_G(Z(G)) \leq N_G(Z(G)) \leq G,$$

so $N_G(Z(G)) = G$. $\square$

2.2: Exercise 5(a). Let $G = S_3$ and $A = \{1, (123), (132)\}$. Show that $C_G(A) = A$ and $N_G(A) = G$.

As General Proposition: In S_3, the 3-cycle subgroup $A = \langle (123) \rangle$ satisfies $C_{S_3}(A) = A$ and $N_{S_3}(A) = S_3$.

As Conditional Proposition: With $G = S_3$ and $A = \{1, (123), (132)\}$, one has $C_G(A) = A$ and $N_G(A) = G$.

. . . .

Intuition. The only elements of S_3 that commute with a 3-cycle are its own powers. Since $|A| = 3$ has index 2 in S_3, A is normal, so the whole group normalizes A.

. . . .

Proof.

Step 1 (Containment). Trivially $A \leq C_G(A)$ and $A \leq N_G(A)$.

Step 2 (Size constraint for $C_G(A)$). By Lagrange, $|C_G(A)|$ divides $|G| = 6$ and is a multiple of $|A| = 3$, so $|C_G(A)| \in \{3, 6\}$.

Step 3 (Not everyone centralizes). A transposition, e.g. (12), does not commute with (123) (compute $(12)(123) = (23) \neq (123)(12) = (13)$). Hence $C_G(A) \neq G$.

Step 4 (Centralizer equals A). From Steps 2–3, $|C_G(A)| = 3$, so $C_G(A) = A$.

Step 5 (Normalizer is G). Since $|G : A| = 2$, $A \lhd G$; equivalently $N_G(A) = G$.

2.2: Exercise 5(b). Let $G = D_8 = \langle r, s \mid r^4 = 1,\ s^2 = 1,\ srs = r^{-1}\rangle$ and $A = \{1, r, r^2, r^3\} = \langle r\rangle$. Show that $C_G(A) = A$ and $N_G(A) = G$.

As General Proposition: In D_8, the rotation subgroup $A = \langle r\rangle$ satisfies $C_{D_8}(A) = A$ and $N_{D_8}(A) = D_8$.

As Conditional Proposition: With $G = D_8$ and $A = \langle r\rangle$, one has $C_G(A) = A$ and $N_G(A) = G$.

. . . .

Intuition. Rotations commute with rotations, but reflections flip r to r^{-1}, so they do not centralize A; nevertheless they *normalize* A because conjugation by a reflection permutes the elements of A.

. . . .

Proof.

Step 1 (Containment). Clearly $A \leq C_G(A) \leq N_G(A) \leq G$.

Step 2 (Size constraint for $C_G(A)$). $|A| = 4$ divides $|C_G(A)|$ and $|C_G(A)| \mid |G| = 8$, so $|C_G(A)| \in \{4, 8\}$.

Step 3 (Reflections do not centralize). Using $srs = r^{-1}$, we have $sr \neq rs$; hence any sr^k fails to commute with r. Thus $C_G(A) \neq G$.

Step 4 (Centralizer equals A). From Steps 2–3, $|C_G(A)| = 4$, so $C_G(A) = A$.

Step 5 (Reflections normalize A). Conjugation $sr^m s = r^{-m}$ permutes A, so $s \in N_G(A)$. Since $A \leq N_G(A)$ and $s \in N_G(A)$, we get $\langle A, s\rangle = D_8 \leq N_G(A)$. Hence $N_G(A) = G$.

2.2: Exercise 5(c). Let $G = D_{10} = \langle r, s \mid r^5 = 1,\ s^2 = 1,\ srs = r^{-1}\rangle$ and $A = \{1, r, r^2, r^3, r^4\} = \langle r\rangle$. Show that $C_G(A) = A$ and $N_G(A) = G$.

As General Proposition: In D_{10}, the rotation subgroup $A = \langle r\rangle$ satisfies $C_{D_{10}}(A) = A$ and $N_{D_{10}}(A) = D_{10}$.

As Conditional Proposition: With $G = D_{10}$ and $A = \langle r\rangle$, one has $C_G(A) = A$ and $N_G(A) = G$.

. . . .

Intuition. As before, reflections fail to commute with r but conjugate r to r^{-1}, keeping A invariant. Since $|A| = 5$ has index 2, A is normal.

. . . .

Proof.

Step 1 (Containment). $A \leq C_G(A) \leq N_G(A) \leq G$.
Step 2 (Size constraint for $C_G(A)$). $|A| = 5$ divides $|C_G(A)|$ and $|C_G(A)| \mid |G| = 10$, so $|C_G(A)| \in \{5, 10\}$.
Step 3 (Not everyone centralizes). Using $srs = r^{-1} \neq r$ (in D_{10}), reflections do not commute with r, so $C_G(A) \neq G$.
Step 4 (Centralizer equals A). Hence $|C_G(A)| = 5$ and $C_G(A) = A$.
Step 5 (Normalizer is G). Since $|G : A| = 2$, $A \lhd G$, so $N_G(A) = G$.

2.2: Exercise 10. Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

As General Proposition: If $|H| = 2$ with $H \leq G$, then $N_G(H) = C_G(H)$. Consequently, if $N_G(H) = G$ then $H \leq Z(G)$.

As Conditional Proposition: Let G be a group and $H \leq G$ with $|H| = 2$. Then $N_G(H) = C_G(H)$; in particular, if $N_G(H) = G$ then $H \subseteq Z(G)$.

. . . .

Intuition. A subgroup of order 2 is $H = \{1, a\}$ with $a^2 = 1$ and $a = a^{-1}$. Conjugation preserves order, so any conjugate of a also has order 2. If an element g normalizes H, the conjugate gag^{-1} must lie in H, hence can only be a (not 1), which means g actually *commutes* with a. Thus "normalizer" collapses to "centralizer" for such H.

. . . .

Proof.

Step 1 (Normalizers land conjugates inside H). Write $H = \{1, a\}$ with $a^2 = 1$. If $g \in N_G(H)$ then $gHg^{-1} = H$, so $gag^{-1} \in H$.

Step 2 (Conjugation preserves order, ruling out 1). The element gag^{-1} has the same order as a, namely 2. Hence $gag^{-1} \neq 1$ and thus $gag^{-1} = a$.

Step 3 (From normalizer to centralizer). From $gag^{-1} = a$ we get $ga = ag$, i.e. $g \in C_G(H)$. Therefore $N_G(H) \subseteq C_G(H)$.

Step 4 (From centralizer to normalizer). Conversely, if $g \in C_G(H)$ then $ga = ag$, so $gHg^{-1} = \{1, gag^{-1}\} = \{1, a\} = H$, hence $g \in N_G(H)$. Therefore $C_G(H) \subseteq N_G(H)$.

Step 5 (Equality). By Steps 3–4, $N_G(H) = C_G(H)$.

Step 6 (Deduction to the center). If $N_G(H) = G$, then $C_G(H) = G$ by Step 5, meaning every $g \in G$ commutes with a. Hence $a \in Z(G)$ and $H \leq Z(G)$.

2.2: Additional Exercise 1 (i) (Transitivity vs. Normality). (i) Show that if K is a subgroup of H and H is a subgroup of G, then K is a subgroup of G. (ii) Exhibit a case where $K \lhd H$ and $H \lhd G$ but $K \ntrianglelefteq G$ by working in the group

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\},$$

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\},$$

$$K = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; b \text{ even} \right\}.$$

As General Proposition: (i) Subgroups are transitive: $K \leq H \leq G \Rightarrow K \leq G$. (ii) In the upper unitriangular integer group G above, $K \lhd H$ and $H \lhd G$ but $K \ntrianglelefteq G$.

As Conditional Proposition: With G, H, K as displayed, we have $K \leq H \leq G$, $K \lhd H$, $H \lhd G$, and $K \ntrianglelefteq G$.

Intuition. (i) If K already satisfies the subgroup conditions inside H, it automatically satisfies them inside G because the operation and inverses are the same. (ii) The group G is the (integer) Heisenberg group. Conjugating

$$g(a,b,c) := \begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}$$

by $g(x,y,z)$ changes b by the shear $b \mapsto b - az$ while keeping c fixed. Hence the condition $c = 0$ (defining H) is stable under all conjugations in G, so $H \triangleleft G$. Inside H (where $z = 0$), conjugation is trivial, so any parity condition on b stays intact ($K \triangleleft H$). But allowing z odd in G can flip the parity of b when a is odd, so K is not normal in G.

Proof (i): $K \leq H \leq G \Rightarrow K \leq G$.
Step 1 (Nonemptiness). Since $K \leq H$, $1 \in K$. As $1 \in G$, $K \neq \varnothing$ in G.
Step 2 (Closure under products). If $x, y \in K$, then $xy \in K$ (because $K \leq H$). Hence $xy \in G$.
Step 3 (Closure under inverses). If $x \in K$, then $x^{-1} \in K$ (since $K \leq H$). Hence $x^{-1} \in G$.
Step 4 (Conclusion). By the subgroup criterion inside G, $K \leq G$.

2.2: Additional Exercise 1 (ii) (Transitivity vs. Normality). (i) Show that if K is a subgroup of H and H is a subgroup of G, then K is a subgroup of G. (ii) Exhibit a case where $K \lhd H$ and $H \lhd G$ but $K \ntrianglelefteq G$ by working in the group

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z} \right\},$$
$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\},$$
$$K = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; b \text{ even} \right\}.$$

As General Proposition: (i) Subgroups are transitive: $K \leq H \leq G \Rightarrow K \leq G$. (ii) In the upper unitriangular integer group G above, $K \lhd H$ and $H \lhd G$ but $K \ntrianglelefteq G$.

As Conditional Proposition: With G, H, K as displayed, we have $K \leq H \leq G$, $K \lhd H$, $H \lhd G$, and $K \ntrianglelefteq G$.

. . . .

Intuition. Write $g(a,b,c) = \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Multiplying shows a shear in the $(1,3)$-entry: $(a,b,c)\cdot(a',b',c') = (a+a',\ b+b'+ac',\ c+c')$. Inverting solves a small linear system. Conjugating $h = (a,b,0) \in H$ by $g = (x,y,z)$ gives $ghg^{-1} = (a,\ b-az,\ 0)$: this preserves $c = 0$ (so $H \lhd G$), fixes b when $z = 0$ (so $K \lhd H$), but can flip the parity of b if z is odd and a is odd (so $K \ntrianglelefteq G$).

. . . .

Proof.

Step 1 (Notation). For integers a, b, c, set $g(a,b,c) = \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}\right)$ and identify it with the triple (a,b,c) for bookkeeping.

Step 2 (Product—explicit multiplication). Compute

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix},$$

since the $(1,3)$-entry is $1\cdot b' + a\cdot c' + b\cdot 1 = b' + ac' + b$ and other entries are immediate; hence $(a,b,c)\cdot(a',b',c') = (a+a',\ b+b'+ac',\ c+c')$.

Step 3 (Inverse—solve $g(a,b,c)g(x,y,z) = I$). Using Step 2,

$$(a,b,c)\cdot(x,y,z) = (a+x,\ b+y+az,\ c+z) = (0,0,0)$$

forces $x = -a$, $z = -c$, and $y = -b + ac$; therefore

$$g(a,b,c)^{-1} = g(-a,\ -b+ac,\ -c) = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}.$$

Step 4 (Conjugation formula—compute $g(x,y,z)\,g(a,b,0)\,g(x,y,z)^{-1}$). First multiply $g(x,y,z)g(a,b,0) = g(x+a,\ y+b,\ z)$ by Step 2; then multiply by $g(-x,\ -b+y+xz,\ -z)$ from Step 3 to get

$$g(x+a,\ y+b,\ z)\,g(-x,\ -y+xz,\ -z) = g\big(a,\ b-az,\ 0\big).$$

Thus $g(x,y,z)\,g(a,b,0)\,g(x,y,z)^{-1} = g(a,\ b-az,\ 0)$.

Step 5 ($H \lhd G$). For any $h = g(a,b,0) \in H$ and any $g = g(x,y,z) \in G$, Step 4 gives $ghg^{-1} = g(a, b-az, 0) \in H$; hence H is normal in G.

Step 6 ($K \lhd H$). If $g \in H$, then $z = 0$ in Step 4, so $ghg^{-1} = g(a,b,0)$ leaves b

unchanged; in particular, "b even" is preserved, so K is normal in H.
Step 7 ($K \ntrianglelefteq G$). Take $h = g(1, 0, 0) \in K$ (here $b = 0$ is even) and $g = g(0, 0, 1) \in G$; Step 4 yields $ghg^{-1} = g(1, -1, 0)$, whose $b = -1$ is odd, so $ghg^{-1} \notin K$; hence K is not normal in G.
Step 8 (Conclusion). We have shown $K \triangleleft H$ and $H \triangleleft G$ but $K \ntrianglelefteq G$, so normality is not transitive in general.

2.4: Exercise 3. Prove that if H is an abelian subgroup of a group G then $\langle H, Z(G) \rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H) \rangle$ is not abelian.

As General Proposition: For any group G and abelian $H \leq G$, the subgroup $\langle H, Z(G) \rangle$ is abelian. Nevertheless, there exist G and abelian $H \leq G$ with $\langle H, C_G(H) \rangle$ nonabelian.

As Conditional Proposition: Let G be a group and $H \leq G$ be abelian. Then $\langle H, Z(G) \rangle$ is abelian. Moreover, in $D_8 = \langle r, s \mid r^4 = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$, the subgroup $H = \{1, r^2\}$ is abelian but $\langle H, C_G(H) \rangle = D_8$ is not abelian.

. . . .

Intuition. Members of the center commute with everything, and members of an abelian subgroup commute with one another. So anything built from H and $Z(G)$ will still commute pairwise, forcing the generated subgroup to be abelian. In contrast, $C_G(H)$ can be much larger than H; in D_8, r^2 is central, so $C_G(H) = D_8$, and the subgroup generated with H is the whole (nonabelian) group.

. . . .

Proof (Abelianness of $\langle H, Z(G)\rangle$).

Step 1 (All generators commute pairwise). If $h, h' \in H$, then $hh' = h'h$ since H is abelian; if $z, z' \in Z(G)$, then $zz' = z'z$ by centrality; if $h \in H$ and $z \in Z(G)$, then $hz = zh$ since z commutes with all elements of G.

Step 2 (Words can be rearranged). Any $g \in \langle H, Z(G)\rangle$ is a finite product of elements from $H \cup Z(G)$. By Step 1, factors may be permuted arbitrarily without changing the product, so any two such words commute.

Step 3 (Conclusion). Therefore every pair of elements of $\langle H, Z(G)\rangle$ commute, i.e. $\langle H, Z(G)\rangle$ is abelian.

Example (An abelian H with $\langle H, C_G(H)\rangle$ nonabelian).

Step 1 (Pick G and H). Let $G = D_8 = \langle r, s \mid r^4 = 1,\ s^2 = 1,\ srs = r^{-1}\rangle$. Take $H = \{1, r^2\} = \langle r^2\rangle$, which is abelian.

Step 2 (Compute the centralizer). Since $r^2 \in Z(D_8)$, every $g \in D_8$ commutes with r^2, so $C_G(H) = G = D_8$.

Step 3 (Generated subgroup). Then $\langle H, C_G(H)\rangle = \langle \{1, r^2\}, D_8\rangle = D_8$.

Step 4 (Nonabelianness). In D_8, $sr \neq rs$ (because $srs = r^{-1}$), hence D_8 is nonabelian, so $\langle H, C_G(H)\rangle$ is not abelian.

2.4: Exercise 14(a). Prove that every finite group is finitely generated.

As General Proposition: Every finite group G admits a finite generating set (for example, G itself).

As Conditional Proposition: Let G be a finite group. Then $G = \langle S \rangle$ for some finite $S \subseteq G$ (e.g. $S = G$).

. . . .

Intuition. A generator set is any subset whose subgroup equals G. For a finite group, taking all elements certainly generates; often a smaller subset works, but existence is immediate.

. . . .

Proof.

Step 1 (Candidate set). Since G is finite, $S := G$ is a finite subset.
Step 2 (Generation). By definition, $\langle S \rangle = \langle G \rangle = G$.
Step 3 (Conclusion). Hence G is finitely generated (indeed, by S).

2.4: Exercise 14(b). Prove that $\mathbb{Z}$ is finitely generated.

As General Proposition: The additive group $\mathbb{Z}$ is cyclic, hence generated by a single element.

As Conditional Proposition: $\mathbb{Z} = \langle 1 \rangle$ (also $\mathbb{Z} = \langle -1 \rangle$).

. . . .

Intuition. Integer addition starts from 1 and repeats: every $n \in \mathbb{Z}$ is 1 added or subtracted finitely many times.

. . . .

Proof.

Step 1 (Containments). $\langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
Step 2 (Exhaustion). For each $n \in \mathbb{Z}$, $n = n \cdot 1 \in \langle 1 \rangle$.
Step 3 (Equality). Thus $\mathbb{Z} = \langle 1 \rangle$, so $\mathbb{Z}$ is finitely generated (by one element).

2.4: Exercise 14(c). Prove that every finitely generated subgroup of $(\mathbb{Q}, +)$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle \frac{1}{k} \rangle$ where k is the product of all denominators appearing in a generating set for H.]

As General Proposition: Every finitely generated subgroup $H \leq (\mathbb{Q}, +)$ is cyclic; in fact $H \leq \left\langle \frac{1}{k} \right\rangle$ for a suitable $k \in \mathbb{Z}_{>0}$.

As Conditional Proposition: If $H = \langle q_1, \ldots, q_m \rangle \leq (\mathbb{Q}, +)$ with $q_i = \frac{a_i}{b_i}$ in lowest terms, set $k := \prod_{i=1}^{m} b_i$. Then $H \leq \left\langle \frac{1}{k} \right\rangle \cong \mathbb{Z}$; hence H is cyclic.

. . . .

Intuition. Clearing denominators by one common multiple turns any integer combination of the generators into an integer multiple of a single unit fraction.

. . . .

Proof.

Step 1 (Normalize generators). Write each $q_i = \frac{a_i}{b_i}$ with $\gcd(a_i, b_i) = 1$ and $b_i > 0$.

Step 2 (Choose a common denominator). Let $k = \prod_{i=1}^{m} b_i \in \mathbb{Z}_{>0}$.

Step 3 (Generic element of H). Any $h \in H$ has the form $h = \sum_{i=1}^{m} n_i q_i = \sum_{i=1}^{m} n_i \frac{a_i}{b_i}$ with $n_i \in \mathbb{Z}$.

Step 4 (Clear denominators). Then

$$h = \sum_{i=1}^{m} n_i \frac{a_i}{b_i} = \sum_{i=1}^{m} n_i a_i \cdot \frac{k}{k b_i} = \left(\sum_{i=1}^{m} n_i a_i \frac{k}{b_i} \right) \cdot \frac{1}{k}.$$

Each $\frac{k}{b_i} \in \mathbb{Z}$, so the coefficient $t := \sum_{i=1}^{m} n_i a_i \frac{k}{b_i} \in \mathbb{Z}$.

Step 5 (Containment). Hence $h = t \cdot \frac{1}{k} \in \left\langle \frac{1}{k} \right\rangle$, so $H \leq \left\langle \frac{1}{k} \right\rangle$.

Step 6 (Cyclicity). Since $\left\langle \frac{1}{k} \right\rangle = \{ \frac{t}{k} \mid t \in \mathbb{Z} \} \cong \mathbb{Z}$ is cyclic, its subgroup H is cyclic.

2.4: Exercise 14(d). Prove that $\mathbb{Q}$ is not finitely generated (as an additive group).

As General Proposition: $(\mathbb{Q}, +)$ is not finitely generated.

As Conditional Proposition: There is no finite subset $S \subset \mathbb{Q}$ with $\langle S \rangle = \mathbb{Q}$.

. . . .

Intuition. If $\mathbb{Q}$ were finitely generated, part (c) would force it to be cyclic, but a single rational cannot generate reciprocals with arbitrarily many distinct prime denominators.

. . . .

Proof.

Step 1 (Assume finite generation). Suppose $\mathbb{Q} = \langle S \rangle$ with S finite. By (c), $\langle S \rangle$ is cyclic, so $\mathbb{Q} = \langle \frac{p}{q} \rangle$ for some relatively prime $p, q \in \mathbb{Z}$, $q \neq 0$.
Step 2 (Pick a new prime). Let r be any prime not dividing q.
Step 3 (Consequence of cyclicity). If $\mathbb{Q} = \langle \frac{p}{q} \rangle$, then $\frac{1}{r}$ must be an integer multiple of $\frac{p}{q}$: there exists $k \in \mathbb{Z}$ with $k\frac{p}{q} = \frac{1}{r}$.
Step 4 (Clear denominators). Then $kp = \frac{q}{r}$, forcing $r \mid q$, which contradicts $\gcd(q, r) = 1$.
Step 5 (Conclusion). The assumption is impossible; therefore $\mathbb{Q}$ is not finitely generated.

2.2: Additional Exercise 2 (i). Suppose $N \leq G$ and N is generated by $T \subseteq N$, while G is generated by $S \subseteq G$.
(i) Prove that if $gTg^{-1} \subseteq N$, then $gNg^{-1} \subseteq N$.
(ii) Prove that if $sNs^{-1} \subseteq N$ for all $s \in S \cup S^{-1}$, then $gNg^{-1} \subseteq N$ for all $g \in G$.
(iii) Deduce that $N \lhd G$ if $sTs^{-1} \subseteq N$ for all $s \in S \cup S^{-1}$.

As General Proposition: Conjugation respects generation: $g\langle T\rangle g^{-1} = \langle gTg^{-1}\rangle$. Hence (i)–(iii) follow by containment and induction on word length in $S \cup S^{-1}$.

As Conditional Proposition: With $N = \langle T\rangle$ and $G = \langle S\rangle$, (i)–(iii) hold as stated.

. . . .

Intuition. Conjugation by a fixed g is an automorphism of G, so it carries generators to generators and generated subgroups to their conjugates. If every generator s (and its inverse) of G conjugates N into itself, then any product of such generators does too—by induction on word length. Finally, if each s even sends the *generators of* N back into N, then each s conjugates N *itself* into N, and the previous step promotes this to all $g \in G$.

. . . .

Proof of (i).

Step 1 (Conjugation distributes over products and inverses). For any $x, y \in G$, $g(xy)g^{-1} = (gxg^{-1})(gyg^{-1})$ and $g(x^{-1})g^{-1} = (gxg^{-1})^{-1}$.

Step 2 (Conjugate of a generated subgroup). Since $N = \langle T \rangle$, every $n \in N$ is a finite word in elements of $T^{\pm 1}$. Applying Step 1 to the word gives gng^{-1} as a word in $(gTg^{-1})^{\pm 1}$, hence

$$gNg^{-1} = g\langle T \rangle g^{-1} = \langle gTg^{-1} \rangle.$$

Step 3 (Containment). If $gTg^{-1} \subseteq N$, then $\langle gTg^{-1} \rangle \subseteq N$, so by Step 2, $gNg^{-1} \subseteq N$.

2.2: Additional Exercise 2 (ii). Suppose $N \leq G$ and N is generated by $T \subseteq N$, while G is generated by $S \subseteq G$.
(i) Prove that if $gTg^{-1} \subseteq N$, then $gNg^{-1} \subseteq N$.
(ii) Prove that if $sNs^{-1} \subseteq N$ for all $s \in S \cup S^{-1}$, then $gNg^{-1} \subseteq N$ for all $g \in G$.
(iii) Deduce that $N \lhd G$ if $sTs^{-1} \subseteq N$ for all $s \in S \cup S^{-1}$.

As General Proposition: Conjugation respects generation: $g\langle T\rangle g^{-1} = \langle gTg^{-1}\rangle$. Hence (i)–(iii) follow by containment and induction on word length in $S \cup S^{-1}$.

As Conditional Proposition: With $N = \langle T\rangle$ and $G = \langle S\rangle$, (i)–(iii) hold as stated.

. . . .

Intuition. Conjugation by a fixed g is an automorphism of G, so it carries generators to generators and generated subgroups to their conjugates. If every generator s (and its inverse) of G conjugates N into itself, then any product of such generators does too—by induction on word length. Finally, if each s even sends the *generators of* N back into N, then each s conjugates N *itself* into N, and the previous step promotes this to all $g \in G$.

. . . .

Proof of (ii).

Step 1 (Goal and strategy). We show by induction on word length ℓ in $S \cup S^{-1}$ that for every word $w = s_1 \cdots s_\ell$ we have $wNw^{-1} \subseteq N$.

Step 2 (Base $\ell = 0, 1$). For $\ell = 0$, $w = 1$ and $wNw^{-1} = N \subseteq N$. For $\ell = 1$, $w = s \in S \cup S^{-1}$, the hypothesis gives $sNs^{-1} \subseteq N$.

Step 3 (Induction step). Write $w = s_1 \cdots s_{\ell-1}\, s_\ell = u\, s_\ell$. Then

$$wNw^{-1} = u\,(s_\ell N s_\ell^{-1})\,u^{-1} \subseteq uNu^{-1}$$

by the hypothesis on s_ℓ. By the induction hypothesis applied to u (length $\ell - 1$), $uNu^{-1} \subseteq N$. Hence $wNw^{-1} \subseteq N$.

Step 4 (Conclusion). Every $g \in G = \langle S \rangle$ is such a word w, so $gNg^{-1} \subseteq N$ for all $g \in G$.

2.2: Additional Exercise 2 (iii). Suppose $N \leq G$ and N is generated by $T \subseteq N$, while G is generated by $S \subseteq G$.
(i) Prove that if $gTg^{-1} \subseteq N$, then $gNg^{-1} \subseteq N$.
(ii) Prove that if $sNs^{-1} \subseteq N$ for all $s \in S \cup S^{-1}$, then $gNg^{-1} \subseteq N$ for all $g \in G$.
(iii) Deduce that $N \lhd G$ if $sTs^{-1} \subseteq N$ for all $s \in S \cup S^{-1}$.

As General Proposition: Conjugation respects generation: $g\langle T\rangle g^{-1} = \langle gTg^{-1}\rangle$. Hence (i)–(iii) follow by containment and induction on word length in $S \cup S^{-1}$.

As Conditional Proposition: With $N = \langle T\rangle$ and $G = \langle S\rangle$, (i)–(iii) hold as stated.

. . . .

Intuition. Conjugation by a fixed g is an automorphism of G, so it carries generators to generators and generated subgroups to their conjugates. If every generator s (and its inverse) of G conjugates N into itself, then any product of such generators does too—by induction on word length. Finally, if each s even sends the *generators of* N back into N, then each s conjugates N *itself* into N, and the previous step promotes this to all $g \in G$.

. . . .

Proof of (iii).

Step 1 (From $sTs^{-1} \subseteq N$ to $sNs^{-1} \subseteq N$). Fix $s \in S \cup S^{-1}$. Since $N = \langle T \rangle$, apply part (i) with $g = s$ to get $sNs^{-1} \subseteq N$.

Step 2 (Promote to all $g \in G$). Now apply part (ii): because $sNs^{-1} \subseteq N$ holds for all $s \in S \cup S^{-1}$, we obtain $gNg^{-1} \subseteq N$ for every $g \in G$.

Step 3 (Normality). Thus $gNg^{-1} \subseteq N$ for all g, and the same applied to g^{-1} yields $N \subseteq gNg^{-1}$, hence $gNg^{-1} = N$; therefore $N \lhd G$.

2.2: Additional Exercise 3. Here is an example of a group G, a subgroup N, and $g \in G$ such that $gNg^{-1} \subseteq N$ but $gNg^{-1} \neq N$. Let $G = \mathrm{Perm}(\mathbb{Z})$ be the permutation group of the set $\mathbb{Z}$. Let $X \subset \mathbb{Z}$ be the set of nonpositive integers $X = \{n \in \mathbb{Z} : \ n \leq 0\}$. Define

$$N = \{\sigma \in G \mid \sigma|_X = \mathrm{id}|_X\}.$$

Let $\tau \in G$ be the translation $\tau(n) = n + 1$. Show that $\tau N \tau^{-1} \subseteq N$ but $\tau N \tau^{-1} \neq N$.

As General Proposition: In $G = \mathrm{Perm}(\mathbb{Z})$ with $X = \{n \leq 0\}$ and $N = \{\sigma : \sigma|_X = \mathrm{id}\}$, the conjugate $\tau N \tau^{-1}$ (where $\tau(n) = n + 1$) is properly contained in N.

As Conditional Proposition: With G, N, X, τ as displayed, we have $\tau N \tau^{-1} \subseteq N$ and $\tau N \tau^{-1} \neq N$.

. . . .

Intuition. Conjugating by τ shifts the "fixed half-line" one step to the right: τ^{-1} moves an input $x \leq 0$ to $x-1 \leq -1$, which is still in X, so any $\sigma \in N$ fixes it; applying τ brings the point back, proving inclusion. But elements of $\tau N \tau^{-1}$ end up fixing both 0 and 1, whereas N contains permutations that move 1 (only the nonpositives must be fixed). Choosing such a permutation shows the inclusion is strict.

. . . .

Proof.

Step 1 (Check inclusion on X). Let $\sigma \in N$ and $x \in X$ with $x \leq 0$. Then $\tau^{-1}(x) = x - 1 \leq -1$, hence $\tau^{-1}(x) \in X$ and $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$. Therefore

$$(\tau\sigma\tau^{-1})(x) = \tau(\tau^{-1}(x)) = x,$$

so $\tau\sigma\tau^{-1}$ fixes every $x \in X$. Thus $\tau N \tau^{-1} \subseteq N$.

Step 2 (A property of all elements in $\tau N \tau^{-1}$). For any $\sigma \in N$ we have

$$(\tau\sigma\tau^{-1})(0) = \tau\sigma(-1) = \tau(-1) = 0, \qquad (\tau\sigma\tau^{-1})(1) = \tau\sigma(0) = \tau(0) = 1,$$

so every element of $\tau N \tau^{-1}$ fixes both 0 and 1.

Step 3 (Exhibit an N-element that moves 1). Define $\pi \in G$ by swapping 1 and 2 and fixing all other integers:

$$\pi(1) = 2,\ \pi(2) = 1,\ \pi(n) = n \text{ for } n \notin \{1, 2\}.$$

Since π fixes every $x \leq 0$, we have $\pi \in N$, but $\pi(1) = 2 \neq 1$.

Step 4 (Strictness). By Step 2, every element of $\tau N \tau^{-1}$ fixes 1, whereas $\pi \in N$ does not; hence $\pi \notin \tau N \tau^{-1}$. Therefore $\tau N \tau^{-1} \subsetneq N$.

Step 5 (Conclusion). We have shown $\tau N \tau^{-1} \subseteq N$ and $\tau N \tau^{-1} \neq N$ as required.