Abstract Algebra in Lean

Louis (Yiyang) Liu

May 14, 2026

Chapter 1

What is a group?

1.1 Definition of a group

A *group* is a pair $(G,\ \cdot)$ — a set G with a binary operation $\cdot : G \times G \to G$ — satisfying:

- *Associativity:* $\forall a, b, c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- *Identity:* $\exists 1 \in G,\ \forall a \in G,\ 1 \cdot a = a$. The $\exists$ is *outside* the $\forall$ — one element acts as identity for *every* a.
- *Inverse:* $\forall a \in G,\ \exists a^{-1} \in G,\ a^{-1} \cdot a = 1$. The $\exists$ is *inside* the $\forall$ — each a has its own inverse.

The Lean class below packages the existential witnesses 1 and $(-)^{-1}$ as named fields via the `One` and `Inv` typeclasses. Mathematically this is the same definition (a chosen witness in place of "some element exists"); the named-witness form lets us write 1 and a^{-1} directly, without extracting them from existentials.

Definition 1. A type G with $\cdot : G \times G \to G$, identity 1, and inverse $(-)^{-1}$ satisfying associativity, left identity $1 \cdot a = a$, and left inverse $a^{-1} \cdot a = 1$. The right-handed duals follow as theorems.

Theorem 2. *Associativity:* $\forall a, b, c,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Proof. □

Theorem 3. *Left identity:* $\forall a,\ 1 \cdot a = a$.

Proof. □

Theorem 4. *Left inverse:* $\forall a,\ a^{-1} \cdot a = 1$.

Proof. □

1.2 Examples

Definition 5. The trivial group: `Unit` with its single element.

Definition 6. $\mathbb{Z}/2\mathbb{Z}$: `Bool` under XOR, identity `false`, every element self-inverse.

1.3 Cancellation, right inverse, right identity

Lemma 7. $a \cdot b = a \cdot c \implies b = c$.

Proof. Left-multiply both sides by a^{-1}, then re-associate. □

Lemma 8. $\forall a,\ a \cdot a^{-1} = 1$.

Proof. Set $b := a \cdot a^{-1}$. Using Theorem 2, Theorem 4, and Theorem 3: $b \cdot b = a(a^{-1}a)a^{-1} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = b$. Then left-multiplying $b \cdot b = b$ by b^{-1}: $b = 1 \cdot b = (b^{-1} \cdot b) \cdot b = b^{-1} \cdot (b \cdot b) = b^{-1} \cdot b = 1$. □

Lemma 9. $\forall a,\ a \cdot 1 = a$.

Proof. Compute $a \cdot 1$ by first substituting $1 = a^{-1} \cdot a$ (the left-inverse axiom Theorem 4), then re-associating to apply $a \cdot a^{-1} = 1$ (Theorem 8):

$$a \cdot 1 = a \cdot (a^{-1} \cdot a) = (a \cdot a^{-1}) \cdot a = 1 \cdot a = a,$$

using Theorem 2 for the second equality and Theorem 3 for the last. □

Lemma 10. $b \cdot a = c \cdot a \implies b = c$.

Proof. Right-multiplying both sides of h by a^{-1} and re-associating, both sides reduce to b and c:

$$b = b \cdot 1 = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = (c \cdot a) \cdot a^{-1} = c \cdot (a \cdot a^{-1}) = c \cdot 1 = c,$$

using Theorem 9, Theorem 8, Theorem 2, and the hypothesis h at the middle equality. □

Lemma 11. $a \cdot b = a \iff b = 1$ *(the second form of the cancellation law).*

Proof. ($\Rightarrow$) Suppose $a \cdot b = a$. By Theorem 9, $a = a \cdot 1$, so $a \cdot b = a \cdot 1$. Left-cancelling a (Theorem 7) gives $b = 1$.

($\Leftarrow$) If $b = 1$, then $a \cdot b = a \cdot 1 = a$ by Theorem 9. □

Lemma 12. $b \cdot a = a \iff b = 1$ *(the dual cancellation statement on the left).*

Proof. ($\Rightarrow$) Suppose $b \cdot a = a$. By Theorem 3, $a = 1 \cdot a$, so $b \cdot a = 1 \cdot a$. Right-cancelling a (Theorem 10) gives $b = 1$.

($\Leftarrow$) If $b = 1$, then $b \cdot a = 1 \cdot a = a$ by Theorem 3. □

1.4 Uniqueness and rearrangement

Lemma 13. $(\forall a,\ e \cdot a = a) \implies e = 1$.

Proof. Specialize the hypothesis h at $a = 1$ to get $e \cdot 1 = 1$. The right-identity lemma Theorem 9 gives $e \cdot 1 = e$. The two equalities together force $e = e \cdot 1 = 1$. □

Lemma 14. *A left inverse and a right inverse of the same element are equal: if $\ell \cdot a = 1$ and $a \cdot r = 1$, then $\ell = r$.*

Proof. Re-write ℓ using Theorem 9, insert $1 = a \cdot r$ from hr, then re-associate with Theorem 2 to expose $\ell \cdot a = 1$ from $h\ell$:

$$\ell = \ell \cdot 1 = \ell \cdot (a \cdot r) = (\ell \cdot a) \cdot r = 1 \cdot r = r,$$

using Theorem 3 for the last equality. □

Lemma 15. $b \cdot a = 1 \implies b = a^{-1}$.

Proof. Starting from b, insert $1 = a \cdot a^{-1}$ (Theorem 8) and re-associate to expose the hypothesis $b \cdot a = 1$:

$$b = b \cdot 1 = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = 1 \cdot a^{-1} = a^{-1},$$

using Theorem 9 for the first equality, Theorem 2 for re-association, the hypothesis h in the middle, and Theorem 3 at the end. □

Lemma 16. $a \cdot b = c \iff a = c \cdot b^{-1}$ — *the basic rearrangement move.*

Proof. The two directions are symmetric right-multiplications.

($\Rightarrow$) Suppose $a \cdot b = c$. Right-multiplying both sides by b^{-1} and re-associating:

$$a = a \cdot 1 = a \cdot (b \cdot b^{-1}) = (a \cdot b) \cdot b^{-1} = c \cdot b^{-1},$$

using Theorem 9, Theorem 8, and Theorem 2.

($\Leftarrow$) Suppose $a = c \cdot b^{-1}$. Right-multiplying both sides by b and re-associating:

$$a \cdot b = (c \cdot b^{-1}) \cdot b = c \cdot (b^{-1} \cdot b) = c \cdot 1 = c,$$

using Theorem 2, Theorem 4, and Theorem 9. □

1.5 Inverses of inverses and of products

Lemma 17. $(a^{-1})^{-1} = a$.

Proof. By Theorem 8, $a \cdot a^{-1} = 1$. Apply the inverse-uniqueness lemma Theorem 15 with the substitution $a \mapsto a^{-1}$ and $b \mapsto a$: its hypothesis reads $b \cdot a = 1$, which in our case is $a \cdot a^{-1} = 1$, and its conclusion $b = a^{-1}$ becomes $a = (a^{-1})^{-1}$. □

Lemma 18. *The identity is its own inverse:* $1^{-1} = 1$.

Proof. By Theorem 3 applied to 1, we have $1 \cdot 1 = 1$. Apply the inverse-uniqueness lemma Theorem 15 with $a \mapsto 1$ and $b \mapsto 1$: its hypothesis $b \cdot a = 1$ reads $1 \cdot 1 = 1$, and its conclusion $b = a^{-1}$ becomes $1 = 1^{-1}$. □

Lemma 19. *The inverse map is injective:* $a^{-1} = b^{-1} \implies a = b$.

Proof. Take the inverse of both sides of h to get $(a^{-1})^{-1} = (b^{-1})^{-1}$. By Theorem 17 applied twice, $(a^{-1})^{-1} = a$ and $(b^{-1})^{-1} = b$, so $a = b$. □

Lemma 20. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Proof. We show $b^{-1} \cdot a^{-1}$ is a left inverse of $a \cdot b$, then apply uniqueness of inverses. Re-associating (Theorem 2) to expose the middle cancellation $a^{-1} \cdot a = 1$ (Theorem 4), then dropping the identity (Theorem 3):

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot 1 \cdot b = b^{-1} \cdot b = 1.$$

Apply Theorem 15 with $a \mapsto a \cdot b$ and $b \mapsto b^{-1} \cdot a^{-1}$: from $b \cdot a = 1$ it concludes $b = a^{-1}$, here giving $b^{-1} \cdot a^{-1} = (a \cdot b)^{-1}$. □

Lemma 21. $(\forall x,\ x \cdot x = 1) \implies G$ *abelian. (Equivalently: a group of exponent* 2 *is commutative.)*

Proof. Fix $a, b \in G$. The proof applies the hypothesis h in three places.

First, at the product $a \cdot b$: $(a \cdot b) \cdot (a \cdot b) = 1$. By Theorem 15, the product is its own inverse: $a \cdot b = (a \cdot b)^{-1}$.

By Theorem 20, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, so $a \cdot b = b^{-1} \cdot a^{-1}$.

Next, apply h at a alone: $a \cdot a = 1$, so by Theorem 15, $a = a^{-1}$. Similarly, h at b yields $b = b^{-1}$.

Combining the three: $a \cdot b = b^{-1} \cdot a^{-1} = b \cdot a$. □

1.6 Natural-number powers

Recursively: $g^0 := 1$ and $g^{n+1} := g^n \cdot g$.

Definition 22. g^n: product of n copies of g on the right of 1.

Lemma 23. $g^0 = 1$.

Proof. □

Lemma 24. $g^{n+1} = g^n \cdot g$.

Proof. □

Lemma 25. $g^{m+n} = g^m \cdot g^n$.

Proof. Induction on n. Base: $g^{m+0} = g^m = g^m \cdot 1 = g^m \cdot g^0$. Step: $g^{m+(n+1)} = g^{(m+n)+1} = g^{m+n} \cdot g = (g^m \cdot g^n) \cdot g = g^m \cdot (g^n \cdot g) = g^m \cdot g^{n+1}$. □

Lemma 26. $(g^m)^n = g^{m \cdot n}$.

Proof. Induction on n. Base: $(g^m)^0 = 1 = g^0 = g^{m \cdot 0}$. Step: $(g^m)^{n+1} = (g^m)^n \cdot g^m = g^{mn} \cdot g^m = g^{mn+m} = g^{m(n+1)}$, using Theorem 25. □

1.7 Order of an element

The order of g is the least positive n with $g^n = 1$. We phrase it as a predicate to avoid committing to a function.

Definition 27. $n > 0 \ \wedge \ g^n = 1 \ \wedge \ (\forall k,\ 0 < k < n \Longrightarrow g^k \neq 1)$.

Lemma 28. IsOrderOf 1 1.

Proof. $1^1 = 1^0 \cdot 1 = 1 \cdot 1 = 1$ (Theorem 24, Theorem 23, Theorem 3); $0 < 1$; and minimality is vacuous (no $k : \mathbb{N}$ has $0 < k < 1$). □

Lemma 29. IsOrderOf $g\, m \ \wedge$ IsOrderOf $g\, n \implies m = n$.

Proof. By trichotomy. If $m < n$, then m is a positive $k < n$ with $g^k = 1$, contradicting the minimality clause of hn. Symmetric for $n < m$. So $m = n$. □

Lemma 30. *If n is the order of g, then $g^m = 1 \iff n \mid m$.*

Proof. ($\Leftarrow$) Suppose $n \mid m$, write $m = kn$. Then $g^m = g^{kn} = (g^n)^k$ by Theorem 26, and $(g^n)^k = 1^k$ since $g^n = 1$ by the second clause of hn. Finally $1^k = 1$ for every $k : \mathbb{N}$, which is a small induction using Theorem 23, Theorem 24, and Theorem 9.

($\Rightarrow$) Conversely, suppose $g^m = 1$. By division with remainder, write $m = qn + r$ with $0 \le r < n$. Then

$$g^m = g^{qn+r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r,$$

using Theorem 25, Theorem 26, and $g^n = 1$. So $g^r = 1$. By the minimality clause of hn (no positive $k < n$ has $g^k = 1$), and the bound $r < n$, the only possibility is $r = 0$. Hence $m = qn$, i.e. $n \mid m$. □

Lemma 31. *Proposition 1.3.6(b) (Nat form): for $k \le \ell$, $g^k = g^\ell \iff \mathrm{ord}(g) \mid (\ell - k)$.*

Proof. Write $\ell = k + (\ell - k)$; since $k \le \ell$, the subtraction $\ell - k$ takes the natural value in $\mathbb{N}$. By Theorem 25,

$$g^\ell = g^{k+(\ell-k)} = g^k \cdot g^{\ell-k}.$$

Therefore $g^k = g^\ell$ holds iff $g^k = g^k \cdot g^{\ell-k}$, and by Theorem 11 that simplifies to $g^{\ell-k} = 1$. Apply Theorem 30 to get the equivalent condition $n \mid (\ell - k)$. □

Lemma 32. *Proposition 1.3.11: if $\mathrm{ord}(g) = n$, then $\mathrm{ord}(g^k) = n/\gcd(n,k)$.*

Proof. Let $d := \gcd(n,k)$, $n' := n/d$, $k' := k/d$. Then $n = dn'$, $k = dk'$, and $\gcd(n',k') = 1$. We must verify the three clauses of $\mathrm{IsOrderOf}\,(g^k)\,n'$.

Positivity. $n' > 0$ since $n > 0$ (the first clause of hn) and $d \mid n$.

Vanishing power. Using Theorem 26 and $g^n = 1$ (from hn):

$$(g^k)^{n'} = g^{kn'} = g^{(dk')(n/d)} = g^{k'n} = (g^n)^{k'} = 1.$$

Equivalently, by Theorem 30, $n \mid kn'$, which is immediate since $kn' = k'n$.

Minimality. Suppose $(g^k)^j = 1$ with $0 < j$. By Theorem 26 and Theorem 30, $g^{kj} = 1$ gives $n \mid kj$, i.e. $dn' \mid dk'j$, i.e. $n' \mid k'j$. Since $\gcd(n',k') = 1$ (Euclid's coprime argument, Theorem 89), we conclude $n' \mid j$, so $j \ge n'$. □

Lemma 33. *Corollary 1.3.12: in $\langle g \rangle$ with $\mathrm{ord}(g) = n$, the power g^k has the same order n — i.e. generates the same cyclic subgroup — iff $\gcd(n,k) = 1$.*

Proof. By Theorem 32, $\mathrm{ord}(g^k) = n/\gcd(n,k)$. Both this and the hypothesised value n are orders of g^k, so by uniqueness of order (Theorem 29), $\mathrm{ord}(g^k) = n$ iff $n/\gcd(n,k) = n$, which (with $n > 0$ from hn) is precisely $\gcd(n,k) = 1$. □

1.8 Permutations

A permutation of α is a bijection $\alpha \to \alpha$. Permutations form a group under composition, non-abelian for $|\alpha| \ge 3$.

Definition 34. A bijection $\alpha \to \alpha$: a forward function paired with a two-sided inverse.

Definition 35. $\sigma \cdot \tau := \sigma \circ \tau$ on Perm α.

Definition 36. $1 :=$ id on Perm α.

Definition 37. σ^{-1}: swap σ.toFun and σ.invFun.

Lemma 38. $\sigma.\mathrm{toFun} = \tau.\mathrm{toFun} \implies \sigma = \tau$.

Proof. Destructure both, substitute h, then show $\sigma.\mathrm{invFun} = \tau.\mathrm{invFun}$ pointwise: $\tau.\mathrm{invFun}\, y = \tau.\mathrm{invFun}(\sigma.\mathrm{toFun}(\sigma.\mathrm{invFun}\, y)) = \sigma.\mathrm{invFun}\, y$. □

Definition 39. $\mathrm{Perm}\,\alpha$ is a group under composition.

Definition 40. The swap on `Bool`: a concrete permutation exchanging `true` and `false`.

Lemma 41. $\mathrm{swap} \cdot \mathrm{swap} = 1$.

Proof. Both sides have forward function $\mathrm{not} \circ \mathrm{not} = \mathrm{id}$; apply Theorem 38. □

1.9 Sign of a permutation

Every permutation of a finite set is a product of *transpositions* (swaps of two elements, fixing the rest). The number of transpositions in such a decomposition is not unique, but its *parity* is. The *sign* of σ, written $\mathrm{sgn}(\sigma)$, is $+1$ when σ is a product of an even number of transpositions (*even*), and -1 otherwise (*odd*).

Sign is a group homomorphism $\mathrm{sgn} : S_n \to \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$. Its kernel is the *alternating group* A_n, the subgroup of even permutations. For $n \geq 5$, A_n is simple — the technical heart of the proof that the quintic is unsolvable by radicals.

A general definition needs finite types and cycle decomposition, deferred to a later chapter. Here we work out the smallest non-trivial case: Perm(Bool), valued in the `Bool` group (`false` $\leftrightarrow +1$, `true` $\leftrightarrow -1$).

Definition 42. Sign of a permutation of `Bool`, valued in `Bool_group`: identity $\mapsto$ `false` $(+1)$; swap $\mapsto$ `true` (-1).

Lemma 43. $\mathrm{sgn}(1) = +1$.

Proof. □

Lemma 44. $\mathrm{sgn}(\mathrm{swap}) = -1$.

Proof. □

Lemma 45. *Sign is a group homomorphism on* $\mathrm{Perm}(\mathrm{Bool})$*:* $\mathrm{sgn}(\sigma \cdot \tau) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau)$ *(the right-hand multiplication is XOR in* `Bool_group`*).*

Proof. $(\sigma \cdot \tau).\mathrm{toFun} = \sigma.\mathrm{toFun} \circ \tau.\mathrm{toFun}$ definitionally. Case-split on $\tau.\mathrm{toFun}\,\mathrm{true}$. If true, identity is direct. If false, use that $\sigma.\mathrm{toFun}$ is injective on `Bool` (via σ.left_inv) to conclude $\sigma.\mathrm{toFun}\,\mathrm{false} =!(\sigma.\mathrm{toFun}\,\mathrm{true})$. □

1.10 Dihedral groups

For $n \geq 1$, the *dihedral group* D_n is the group of rigid symmetries of a regular n-gon. It has $2n$ elements: n rotations $1, r, r^2, \ldots, r^{n-1}$ and n reflections $s, rs, r^2s, \ldots, r^{n-1}s$, where r is rotation by $2\pi/n$ and s is a fixed reflection. The generators satisfy

$$r^n = 1, \qquad s^2 = 1, \qquad s \cdot r = r^{-1} \cdot s,$$

and these three relations characterize D_n up to isomorphism: every element is uniquely of the form $r^k s^\varepsilon$ with $0 \leq k < n$ and $\varepsilon \in \{0, 1\}$. D_n is non-abelian for $n \geq 3$.

Rather than constructing a concrete model, we abstract the presentation as a typeclass `IsDihedral`: distinguished generators (r, s) in a group G satisfying the three relations.

Definition 46. A dihedral presentation of degree n on G: distinguished generators r, s with $r^n = 1$, $s^2 = 1$, and $s \cdot r = r^{-1} \cdot s$.

Definition 47. Distinguished rotation $r \in G$.

Definition 48. Distinguished reflection $s \in G$.

Theorem 49. $r^n = 1$.

Proof. □

Theorem 50. $s^2 = 1$.

Proof. □

Theorem 51. $s \cdot r = r^{-1} \cdot s$.

Proof. □

Lemma 52. $s = s^{-1}$*: the reflection is an involution.*

Proof. $s \cdot s = 1$ (Theorem 50) and Theorem 15 give $s = s^{-1}$. □

1.11 Abelian groups

A group is *abelian* if $\forall a, b,\ a \cdot b = b \cdot a$. Contrast with Perm($\alpha$) above, non-abelian for $|\alpha| \geq 3$.

Definition 53. A group with $\forall a, b,\ a \cdot b = b \cdot a$.

Theorem 54. *Commutativity:* $\forall a, b,\ a \cdot b = b \cdot a$.

Proof. □

Definition 55. `Bool` is abelian (the smallest non-trivial abelian group, $\mathbb{Z}/2\mathbb{Z}$).

Lemma 56. $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ *in an abelian group.*

Proof. Theorem 20: $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$; then commute via Theorem 54. □

Lemma 57. $g \cdot h \cdot g^{-1} = h$ *in an abelian group (conjugation is trivial).*

Proof. Commute g past h, re-associate, then $g \cdot g^{-1} = 1$ and $h \cdot 1 = h$. □

Lemma 58. $(g \cdot h)^n = g^n \cdot h^n$ *in an abelian group.*

Proof. Induction on n; the step uses commutativity to slide a single g past h^n. □

1.12 Subgroups

A *subgroup* of G is a subset $H \subseteq G$ that is a group under the operation of G: $1 \in H$, H is closed under $\cdot$ and under $(-)^{-1}$. We package H as a predicate `carrier` with these three closure conditions.

Definition 59. A predicate $H : G \to \mathrm{Prop}$ with $1 \in H$, closed under $\cdot$ and $(-)^{-1}$.

Definition 60. $\top := G$ (the whole group as a subgroup of itself).

Definition 61. $\bot := \{1\}$ (the trivial subgroup).

Definition 62. $H \cap K$ is a subgroup.

Lemma 63. *Subgroup criterion: a non-empty $P : G \to \mathrm{Prop}$ closed under $a, b \mapsto a \cdot b^{-1}$ is a subgroup. (One-shot test in place of checking $1 \in P$, closure under $\cdot$, closure under $(-)^{-1}$ separately.)*

Proof. Pick x with $P\,x$. Then $1 = x \cdot x^{-1} \in P$ (Theorem 8). From $P\,1$ and $P\,a$: $a^{-1} = 1 \cdot a^{-1} \in P$ (Theorem 3). From $P\,a$ and $P\,b^{-1}$: $a \cdot b = a \cdot (b^{-1})^{-1} \in P$ (Theorem 17). □

1.13 Subgroups generated by a subset

Given $U \subseteq G$, the *subgroup generated by* U, written $\langle U \rangle$, is the smallest subgroup of G containing U. We build it inductively as the closure of U under 1, $\cdot$, and $(-)^{-1}$, then check the universal property: any subgroup of G containing U contains $\langle U \rangle$. Equivalently, $\langle U \rangle$ is the intersection of all subgroups of G containing U. The single-element case $\langle \{g\} \rangle$ specializes to Theorem 70.

Definition 64. Closure of U under 1, $\cdot$ and $(-)^{-1}$ — the underlying predicate of $\langle U \rangle$.

Definition 65. $\langle U \rangle$: the subgroup generated by $U \subseteq G$.

Lemma 66. $U \subseteq \langle U \rangle$.

Proof. □

Lemma 67. *$\langle U \rangle$ is the smallest subgroup containing U: $U \subseteq H \implies \langle U \rangle \subseteq H$.*

Proof. Induction on the inductive predicate Closure U: the four constructors match exactly the four closure conditions of `MySubgroup`. □

Definition 68. The intersection of an arbitrary family of subgroups is a subgroup.

1.14 Cyclic subgroups

The *cyclic subgroup generated by* g, written $\langle g \rangle$, is the smallest subgroup of G containing g; equivalently it is $\{\, g^n : n \in \mathbb{Z} \,\}$. We build $\langle g \rangle$ inductively as the closure of $\{g\}$ under 1, $\cdot$, and $(-)^{-1}$. A group is *cyclic* if $G = \langle g \rangle$ for some g.

Definition 69. The closure of $\{g\}$ under 1, $\cdot$, and $(-)^{-1}$ — the underlying predicate of $\langle g \rangle$.

Definition 70. $\langle g \rangle$: the cyclic subgroup generated by g.

Lemma 71. $g \in \langle g \rangle$.

Proof. □

Lemma 72. $\forall n : \mathbb{N},\ g^n \in \langle g \rangle$.

Proof. Induction on n. Base: $g^0 = 1 \in \langle g \rangle$. Step: $g^{n+1} = g^n \cdot g$ with $g^n, g \in \langle g \rangle$. □

Lemma 73. *Proposition 1.3.3: $\langle g \rangle$ is the smallest subgroup containing g. Concretely: any subgroup H containing g also contains $\langle g \rangle$.*

Proof. Induction on $(\text{cyclic}\, g).\text{carrier}\, x$, i.e. on the inductive predicate $\text{Generated}\, g$. The four constructors of $\text{Generated}\, g$ correspond exactly to the four closure conditions of H:

- $g \in H$ is the hypothesis hg;
- $1 \in H$ by H.one_mem;
- closure under $\cdot$ by H.mul_mem;
- closure under $(-)^{-1}$ by H.inv_mem.

So each step of the induction stays inside H. □

Definition 74. $\exists g \in G,\ \forall x \in G,\ x \in \langle g \rangle$ (i.e. $G = \langle g \rangle$ for some g).

Lemma 75. *Proposition 1.3.14(a): every subgroup of a cyclic group is cyclic.*

Stated for a subgroup $H \subseteq \langle g \rangle$ of an ambient cyclic-style subgroup: there exists $g' \in H$ such that $H = \langle g' \rangle$ — i.e. H is itself cyclic, generated by some element of H.

Proof. Two cases on whether H is trivial.

Case 1: $H = \{1\}$. Take $g' := 1$. Then $g' \in H$ by `MySubgroup.one_mem`, and $\langle 1 \rangle = \{1\}$ (the inductive closure of $\{1\}$ is generated only by 1), which agrees with H.

Case 2: $H \neq \{1\}$. Since $H \subseteq \langle g \rangle$, every $h \in H$ has the form $h = g^m$ for some $m \in \mathbb{Z}$ (informally; or some $g^m \cdot g^{-m'}$ via the inductive Generated). H contains some non-identity element, hence some g^m with $m \neq 0$; closure of H under $(-)^{-1}$ produces a positive-exponent element. Let k be the smallest positive integer with $g^k \in H$ (well-ordering). Take $g' := g^k$.

Closure of H under $\cdot$ and $(-)^{-1}$ gives every $g^{jk} \in H$ for $j \in \mathbb{Z}$, so $\langle g^k \rangle \subseteq H$. Conversely, fix any $h = g^m \in H$ and divide $m = qk + r$ with $0 \leq r < k$. Then $g^r = g^m \cdot (g^k)^{-q}$ is a product of elements of H, hence in H. Minimality of k and $0 \leq r < k$ force $r = 0$, so $g^m = (g^k)^q \in \langle g^k \rangle$. □

1.15 Subgroups of $(\mathbb{Z}, +)$

The additive group $(\mathbb{Z}, +)$ has a particularly transparent subgroup structure: every subgroup equals $a\mathbb{Z} := \{\, ka : k \in \mathbb{Z} \,\}$ for a unique $a \geq 0$. This single classification underwrites gcd, lcm, Bézout's identity, and the elementary divisibility theory of $\mathbb{Z}$.

We have only developed the multiplicative `MyGroup`, so we spell out the closure conditions for $(\mathbb{Z}, +)$ directly as a predicate `IsAddSubgroupZ`.

Definition 76. $S \subseteq \mathbb{Z}$ is an additive subgroup of $(\mathbb{Z}, +)$: closed under 0, $+$, and negation.

Definition 77. $a\mathbb{Z} := \{\, ka : k \in \mathbb{Z} \,\}$.

Lemma 78. *$a\mathbb{Z}$ is an additive subgroup of $(\mathbb{Z}, +)$.*

Proof. $(ka) + (k'a) = (k + k')a$.
$-(ka) = (-k)a$. □

Theorem 79. *Classification of subgroups of $(\mathbb{Z}, +)$: every additive subgroup equals $a\mathbb{Z}$ for some $a \geq 0$.*

Proof. If $S = \{0\}$, take $a = 0$. Otherwise S contains some nonzero n; closure under negation gives $|n| > 0 \in S$, so $\{n \in S : n > 0\}$ is non-empty. Let a be its least element (well-ordering). Closure under $+$ and negation gives $a\mathbb{Z} \subseteq S$. For $S \subseteq a\mathbb{Z}$, take $n \in S$ and write $n = qa + r$ with $0 \leq r < a$ (division with remainder); then $r = n - qa \in S$, and by minimality $r = 0$, so $a \mid n$. □

1.16 gcd and lcm

Two additive subgroups built from $a, b \in \mathbb{Z}$ carry most of elementary number theory:

$$a\mathbb{Z} + b\mathbb{Z} := \{\, ra + sb : r, s \in \mathbb{Z} \,\}, \qquad a\mathbb{Z} \cap b\mathbb{Z}.$$

Applying Theorem 79, each equals $d\mathbb{Z}$ for a unique $d \geq 0$; the two values are $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ respectively. From this characterization, divisibility properties, Bézout's identity, and the formula $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |ab|$ are immediate.

Definition 80. $a\mathbb{Z} + b\mathbb{Z} := \{\, ra + sb : r, s \in \mathbb{Z} \,\}$.

Lemma 81. *$a\mathbb{Z} + b\mathbb{Z}$ is an additive subgroup of $(\mathbb{Z}, +)$.*

Proof. □

Lemma 82. *$a\mathbb{Z} \cap b\mathbb{Z}$ is an additive subgroup of $(\mathbb{Z}, +)$.*

Proof. □

Definition 83. d is *a* gcd of a, b: $d \geq 0$ and $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

Definition 84. m is *an* lcm of a, b: $m \geq 0$ and $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Lemma 85. *Bézout:* $d = \gcd(a, b) \implies \exists r, s : ra + sb = d$.

Proof. $d = 1 \cdot d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ gives the desired r, s. □

Lemma 86. $d = \gcd(a, b) \implies d \mid a \ \wedge \ d \mid b$.

Proof. $a = 1 \cdot a + 0 \cdot b \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, so $d \mid a$; symmetrically $d \mid b$. □

Lemma 87. *Universality of* gcd*: any common divisor of a, b divides* $\gcd(a, b)$.

Proof. Theorem 85: $\exists r, s : ra + sb = d$. $e \mid a \ \wedge \ e \mid b \implies e \mid ra + sb = d$. □

Definition 88. a, b are *coprime* if $\gcd(a, b) = 1$.

Lemma 89. *a, b coprime* $\iff \exists r, s : ra + sb = 1$.

Proof. ($\Rightarrow$) Theorem 85 with $d = 1$. ($\Leftarrow$) $ra + sb = 1$ puts 1 in $a\mathbb{Z} + b\mathbb{Z}$; so $\mathbb{Z} = 1\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$; the reverse inclusion is automatic. □

Theorem 90. *Euclid's lemma: p prime, $p \mid ab \implies p \mid a \ \vee \ p \mid b$.*

Proof. Suppose $p \nmid a$. Since the only positive divisors of p are 1 and p, $\gcd(a, p) = 1$. By Theorem 89, $\exists r, s : ra + sp = 1$; multiplying by b yields $rab + spb = b$, and p divides both summands, hence b. □

Lemma 91. *If $m = \mathrm{lcm}(a, b)$, then both a and b divide m (Proposition 1.2.7(a)).*

Proof. By definition of IsLcm, $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, and $m \in m\mathbb{Z}$ (via $m = 1 \cdot m$). So $m \in a\mathbb{Z}$, meaning there is some k with $m = ka$; this is precisely $a \mid m$. Symmetrically, $m \in b\mathbb{Z}$ gives $b \mid m$. □

Lemma 92. *Universality of* lcm*: if $a \mid n$ and $b \mid n$, then $\mathrm{lcm}(a, b) \mid n$ (Proposition 1.2.7(b)).*

Proof. $a \mid n$ says $n \in a\mathbb{Z}$ and $b \mid n$ says $n \in b\mathbb{Z}$, so $n \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, which is precisely $m \mid n$. □

Theorem 93. $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = |a \cdot b|$ *for a, b both nonzero (Corollary 1.2.8).*

Proof. By Theorem 86, $d \mid a$ and $d \mid b$, so a/d and b/d are integers and ab/d is a common multiple of a and b. By the universality of lcm (Theorem 92), $m \mid ab/d$, hence $dm \mid ab$.

Conversely, write $d = ra + sb$ (Theorem 85). By Theorem 91, $a \mid m$ and $b \mid m$, so $m = at = bu$ for some integers t, u. Then

$$dm = ram + sbm = (ra)(bu) + (sb)(at) = ab \cdot (ru + st),$$

so $ab \mid dm$.

Each of dm and ab divides the other, so they agree up to sign: $|dm| = |ab|$. Since $d, m \geq 0$ (definitions of IsGcd, IsLcm), $dm \geq 0$, and we conclude $d \cdot m = |a \cdot b|$. □

1.17 Group homomorphisms

A *group homomorphism* $\varphi : G \to G'$ is a function compatible with multiplication: $\forall a, b \in G$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Two consequences follow from this single axiom: $\varphi(1) = 1$ (Theorem 97) and $\varphi(a^{-1}) = \varphi(a)^{-1}$ (Theorem 98).

Standard examples (left informal here for lack of infrastructure): $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$, $\mathrm{sgn} : S_n \to \{\pm 1\}$, $\exp : (\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot)$, the power map $\psi_a : (\mathbb{Z}, +) \to (G, \cdot)$, $n \mapsto a^n$, and $|\cdot| : (\mathbb{R}^\times, \cdot) \to (\mathbb{R}^\times, \cdot)$.

Definition 94. A group homomorphism $\varphi : G \to G'$.

Definition 95. Underlying function $G \to G'$.

Theorem 96. *Multiplicativity: $\forall a, b,\ \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.*

Proof. □

Lemma 97. $\varphi(1) = 1$*: homomorphisms preserve the identity.*

Proof. Start from the identity $1 = 1 \cdot 1$ in G (Theorem 3). Applying φ and using multiplicativity Theorem 96 gives

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1).$$

Rewriting the left-hand side as $\varphi(1) = \varphi(1) \cdot 1$ (Theorem 9):

$$\varphi(1) \cdot \varphi(1) = \varphi(1) \cdot 1.$$

Cancelling $\varphi(1)$ on the left (Theorem 7) yields $\varphi(1) = 1$. □

Lemma 98. $\varphi(a^{-1}) = \varphi(a)^{-1}$*: homomorphisms preserve inverses.*

Proof. We show $\varphi(a^{-1})$ is a left inverse of $\varphi(a)$, then apply uniqueness of inverses. Using multiplicativity Theorem 96, the left-inverse axiom Theorem 4, and identity preservation Theorem 97:

$$\varphi(a^{-1}) \cdot \varphi(a) = \varphi(a^{-1} \cdot a) = \varphi(1) = 1.$$

Now Theorem 15 (with $a \mapsto \varphi(a)$ and $b \mapsto \varphi(a^{-1})$) concludes $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Lemma 99. *$\varphi(a^n) = \varphi(a)^n$ for $n : \mathbb{N}$: homomorphisms preserve natural-number powers.*

Proof. Induction on n.

Base ($n = 0$): by Theorem 23 both sides reduce to the identity:

$$\varphi(a^0) = \varphi(1) = 1 = \varphi(a)^0,$$

using Theorem 97 for the middle equality.

Step ($n \mapsto n + 1$): assume $\varphi(a^n) = \varphi(a)^n$. By Theorem 24, $a^{n+1} = a^n \cdot a$; multiplicativity Theorem 96 and the inductive hypothesis yield

$$\varphi(a^{n+1}) = \varphi(a^n \cdot a) = \varphi(a^n) \cdot \varphi(a) = \varphi(a)^n \cdot \varphi(a) = \varphi(a)^{n+1},$$

with the last equality again by Theorem 24. □

Definition 100. The trivial homomorphism $\tau : G \to G'$, $x \mapsto 1$.

Definition 101. The identity homomorphism $\mathrm{id}_G : G \to G$.

1.18 Image, kernel, and the kernel test

Two subgroups attached to $\varphi : G \to G'$:

$$\operatorname{im}\varphi := \{\, \varphi(a) : a \in G \,\} \subseteq G', \qquad \ker\varphi := \{\, a \in G : \varphi(a) = 1 \,\} \subseteq G.$$

The kernel is more than a subgroup — it is *normal* in G (Theorem 118). Injectivity of φ reduces to triviality of the kernel (Theorem 105).

Definition 102. $\operatorname{im}\varphi$ as a subgroup of G'.

Definition 103. $\ker\varphi$ as a subgroup of G.

Lemma 104. *Kernel test: $\varphi(a) = \varphi(b) \iff a^{-1} \cdot b \in \ker\varphi$.*

Proof. A chain of equivalences. The first is cancellation in G': $\varphi(a) = \varphi(b)$ holds iff multiplying both sides on the left by $\varphi(a)^{-1}$ gives the same thing, i.e. iff $\varphi(a)^{-1} \cdot \varphi(b) = 1$. The second uses Theorem 98 to rewrite $\varphi(a)^{-1} = \varphi(a^{-1})$. The third uses multiplicativity Theorem 96 to combine the two factors into one application of φ:

$$\varphi(a) = \varphi(b) \iff \varphi(a)^{-1} \cdot \varphi(b) = 1 \iff \varphi(a^{-1}) \cdot \varphi(b) = 1 \iff \varphi(a^{-1} \cdot b) = 1.$$

The last condition is exactly $a^{-1} \cdot b \in \ker\varphi$. □

Lemma 105. *φ injective $\iff \ker\varphi = \{1\}$.*

Proof. ($\Rightarrow$) Assume φ is injective and let $a \in \ker\varphi$, i.e. $\varphi(a) = 1$. Since $\varphi(1) = 1$ (Theorem 97), $\varphi(a) = \varphi(1)$. Injectivity gives $a = 1$.

($\Leftarrow$) Assume $\ker\varphi = \{1\}$ and let $a, b \in G$ with $\varphi(a) = \varphi(b)$. By the kernel test Theorem 104, $a^{-1} \cdot b \in \ker\varphi$, so $a^{-1} \cdot b = 1$. Left-multiplying by a and simplifying with Theorem 8 and Theorem 3 (or via mul_eq_iff_eq_mul_inv rearrangements): $b = a$. □

Definition 106. Composition of homomorphisms is a homomorphism: $(\psi \circ \varphi)(a) := \psi(\varphi(a))$.

Definition 107. Image of a subgroup $H \leq G$ under φ: $\varphi(H) := \{\, \varphi(h) : h \in H \,\} \leq G'$. Specializes to Theorem 102 at $H = \top$.

Definition 108. Preimage of a subgroup $K \leq G'$ under φ: $\varphi^{-1}(K) := \{\, x \in G : \varphi(x) \in K \,\} \leq G$. Specializes to Theorem 103 at $K = \bot$.

1.19 Isomorphisms

A *group isomorphism* $\varphi : G \xrightarrow{\sim} G'$ is a bijective homomorphism. Two groups are *isomorphic*, written $G \cong G'$, if there exists an isomorphism between them. Isomorphism is an equivalence relation on groups: reflexive via Theorem 113, symmetric by swapping toFun and invFun, and transitive by composing the underlying homomorphisms.

Definition 109. A group isomorphism: a homomorphism bundled with a two-sided inverse function.

Definition 110. Two-sided inverse function $G' \to G$.

Theorem 111. *Left inverse:* $\forall x,\ \mathrm{invFun}(\mathrm{toFun}\, x) = x$.

Proof. □

Theorem 112. *Right inverse:* $\forall y,\ \mathrm{toFun}(\mathrm{invFun}\, y) = y$.

Proof. □

Definition 113. The identity isomorphism $\mathrm{id}_G : G \xrightarrow{\sim} G$.

Definition 114. The inverse isomorphism $e^{-1} : G' \xrightarrow{\sim} G$.

Definition 115. Composition of isomorphisms is an isomorphism.

1.20 Normal subgroups

A subgroup $H \leq G$ is *normal*, written $H \lhd G$, if $\forall g \in G, h \in H,\ g \cdot h \cdot g^{-1} \in H$. Two key facts: every kernel is normal (Theorem 118), and in an abelian group every subgroup is normal (Theorem 117). The converse to the first — every normal subgroup is the kernel of a homomorphism $G \to G/N$ — is true but requires quotient groups, deferred to a later chapter.

Definition 116. $H \lhd G$: $\forall g \in G, h \in H,\ g \cdot h \cdot g^{-1} \in H$.

Lemma 117. *In an abelian group, every subgroup is normal.*

Proof. $g \cdot h \cdot g^{-1} = h$ in an abelian group (Theorem 57). □

Lemma 118. *Kernels are normal:* $\ker\varphi \lhd G$.

Proof. Fix $g \in G$ and $h \in \ker\varphi$ (so $\varphi(h) = 1$). We show $g \cdot h \cdot g^{-1} \in \ker\varphi$ by direct computation. Multiplicativity Theorem 96 and the inverse-preservation lemma Theorem 98 give

$$\varphi(g \cdot h \cdot g^{-1}) = \varphi(g) \cdot \varphi(h) \cdot \varphi(g^{-1}) = \varphi(g) \cdot \varphi(h) \cdot \varphi(g)^{-1}.$$

Substituting $\varphi(h) = 1$ and simplifying with Theorem 3 (or Theorem 9) and Theorem 8:

$$\varphi(g) \cdot 1 \cdot \varphi(g)^{-1} = \varphi(g) \cdot \varphi(g)^{-1} = 1.$$

Hence $g \cdot h \cdot g^{-1} \in \ker\varphi$. □

Lemma 119. *Preimage of a normal subgroup under a homomorphism is normal:* $K \lhd G' \implies \varphi^{-1}(K) \lhd G$.

Proof. For $g \in G$ and $h \in \varphi^{-1}(K)$ (i.e. $\varphi(h) \in K$), $\varphi(ghg^{-1}) = \varphi(g) \cdot \varphi(h) \cdot \varphi(g)^{-1} \in K$ by $K \lhd G'$, so $ghg^{-1} \in \varphi^{-1}(K)$. □

Lemma 120. *The trivial subgroup is normal.*

Proof. $h = 1 \implies g \cdot 1 \cdot g^{-1} = g \cdot g^{-1} = 1$ via Theorem 9 and Theorem 8. □

Lemma 121. *The whole group is normal in itself.*

Proof. Membership in $\top$ is trivially `True`. □

Lemma 122. *Intersection of two normal subgroups is normal.*

Proof. $h \in H \cap K \implies h \in H$ and $h \in K$, so $ghg^{-1} \in H$ and $ghg^{-1} \in K$, hence $ghg^{-1} \in H \cap K$. □

1.21 The center

The *center* of G is the set of elements that commute with every element of G:

$$Z(G) := \{\, z \in G : \forall x \in G,\ z \cdot x = x \cdot z \,\}.$$

The center captures the "abelian part" of G: by inspection, G is abelian if and only if $Z(G) = G$ (Theorem 124). Beyond this, $Z(G)$ is always a normal subgroup of G (Theorem 125), which makes it a natural source of structure information about non-abelian groups. Its construction is the prototype for the centralizer of a single element (Theorem 126), since unwinding definitions gives $Z(G) = \bigcap_{a \in G} C_G(a)$.

Definition 123. $Z(G) := \{\, z : \forall x,\ z \cdot x = x \cdot z \,\}$, the center of G, as a subgroup.

Lemma 124. *G is abelian* $\iff Z(G) = G$.

Proof. Unfolding $(z \in Z(G))$ to $\forall x,\ zx = xz$, both sides are literally the same statement $\forall z, x \in G,\ z \cdot x = x \cdot z$ — the first quantified over z first, the second over a first, but the underlying universal statement is the same. □

Lemma 125. *The center is a normal subgroup:* $Z(G) \lhd G$.

Proof. Fix $z \in Z(G)$ and $g \in G$; we must show that gzg^{-1} commutes with every element of G. Let $x \in G$ be arbitrary.

The key step is to insert $1 = g^{-1}g$ in the middle of $(gzg^{-1}) \cdot x$, then commute z past $g^{-1}xg$ using $z \in Z(G)$:

$$\begin{aligned}(gzg^{-1}) \cdot x &= g \cdot z \cdot (g^{-1} \cdot x \cdot g) \cdot g^{-1} && \text{(insert } g^{-1}g = 1 \text{ and re-associate)}\\ &= g \cdot (g^{-1} \cdot x \cdot g) \cdot z \cdot g^{-1} && (z \in Z(G), \text{ applied to } g^{-1}xg)\\ &= x \cdot (gzg^{-1}) && (\text{cancel } gg^{-1} = 1).\end{aligned}$$

The first and last lines use Theorem 2, Theorem 4, Theorem 8, Theorem 3, and Theorem 9 to perform the insertion and cancellation. Hence $gzg^{-1} \in Z(G)$. □

1.22 Centralizer, normalizer, and inner automorphisms

Generalizing the center, we attach two subgroups and one homomorphism to a given element or subgroup of G.

The *centralizer* of $a \in G$ is the set of elements that commute with a,

$$C_G(a) := \{\, g \in G : g \cdot a = a \cdot g \,\}.$$

This is a subgroup of G, and unfolding definitions shows that the center is the intersection of all centralizers: $Z(G) = \bigcap_{a \in G} C_G(a)$.

The *normalizer* of a subgroup $H \leq G$ is the set of elements whose conjugation action stabilizes H as a set,

$$N_G(H) := \{\, g \in G : \forall h \in G,\ h \in H \iff ghg^{-1} \in H \,\}.$$

This is again a subgroup of G. Every element of H already satisfies the condition — conjugation by $h \in H$ keeps things inside the subgroup — so $H \subseteq N_G(H)$ (Theorem 129). The normalizer characterizes normality:

$$H \lhd G \iff N_G(H) = G$$

(Theorem 130).

For each fixed $g \in G$, the conjugation map

$$\mathrm{conj}_g : G \to G, \qquad x \mapsto g \cdot x \cdot g^{-1},$$

is a group homomorphism — an *inner automorphism* of G.

Definition 126. $C_G(a) := \{\, g \in G : g \cdot a = a \cdot g \,\}$, the centralizer of a, as a subgroup of G.

Definition 127. For each $g \in G$, conjugation by g, $\mathrm{conj}_g : G \to G$, $x \mapsto g \cdot x \cdot g^{-1}$, is a group homomorphism (an *inner automorphism* of G).

Definition 128. $N_G(H) := \{\, g : \forall h,\ h \in H \iff ghg^{-1} \in H \,\}$, the normalizer of H in G, as a subgroup.

Lemma 129. *Every subgroup is contained in its own normalizer: $H \subseteq N_G(H)$.*

Proof. Fix $h \in H$ and an arbitrary $h' \in G$; we show $h' \in H \iff h \cdot h' \cdot h^{-1} \in H$.

($\Rightarrow$) If $h' \in H$, then since $h \in H$, $h^{-1} \in H$ (by `MySubgroup.inv_mem`), and H is closed under multiplication (by `MySubgroup.mul_mem`), the product $h \cdot h' \cdot h^{-1}$ lies in H.

($\Leftarrow$) Conversely, suppose $h \cdot h' \cdot h^{-1} \in H$. Conjugating by h^{-1} — which also lies in H — and using Theorem 17 to identify $(h^{-1})^{-1}$ with h:

$$h' = h^{-1} \cdot (h \cdot h' \cdot h^{-1}) \cdot (h^{-1})^{-1} \in H,$$

again by closure of H under multiplication. □

Lemma 130. *H is normal in G iff its normalizer is all of G: $H \lhd G \iff \forall g \in G,\ g \in N_G(H)$.*

Proof. Both sides assert: $\forall g, h,\ h \in H \iff ghg^{-1} \in H$.

($\Rightarrow$) Assume $H \lhd G$. Fix $g \in G$ and $h \in G$. The forward implication $h \in H \implies ghg^{-1} \in H$ is the definition of $H \lhd G$. For the reverse, suppose $ghg^{-1} \in H$. Apply normality with g^{-1} in place of g to the element ghg^{-1}:

$$g^{-1} \cdot (ghg^{-1}) \cdot (g^{-1})^{-1} = h \in H,$$

using Theorem 17 to rewrite $(g^{-1})^{-1} = g$.

($\Leftarrow$) Conversely, if every $g \in G$ lies in $N_G(H)$, then in particular the forward direction of the biconditional gives $h \in H \implies ghg^{-1} \in H$ for every $g \in G$ — which is exactly $H \lhd G$. □