Groups

Table of contents

The definition . . . 1
Commutative and abelian . . . 2
Associativity is about brackets, not order . . . 3
Checking the four properties . . . 3
Eight candidates . . . 4
A group of functions: $ax + b$ . . . 6
Why these four: solving equations . . . 7
Elementary properties . . . 8
Common mistakes . . . 10
See also . . . 10

A group is a set together with one operation on it that satisfies four properties: closure, associativity, identity and inverses. The four are enough to solve any equation $a * x = b$. The course's examples are numbers under addition, non-zero real numbers under multiplication, the classes of integers-modulo-n[1], and the bijections of the symmetric-group[2] under composition. A small group is checked from its table (cayley-tables[3]). Groups inside groups, and the powers of an element, are in subgroups-and-cyclic-groups[4]. First met in 2026-09-24-definitions-and-examples-of-groups[5], and continued in 2026-10-06-elementary-properties-of-groups[6].

The definition

> **Definition**: If G is a set and $*$ is a binary operation on G, then $(G, *)$ is a **group** if it has the following properties:-

[1] courses/math1061/integers-modulo-n.pdf
[2] courses/math1061/symmetric-group.pdf
[3] courses/math1061/cayley-tables.pdf
[4] courses/math1061/subgroups-and-cyclic-groups.pdf
[5] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[6] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

(1) Closure: for all $g, h \in G$, $g * h \in G$.

(2) Associativity: for all $g, h, k \in G$, $(g * h) * k = g * (h * k)$.

(3) Identity: $\exists e \in G$ such that $\forall g \in G$, $e * g = g * e = g$.

(4) Inverses: $\forall g \in G$, $\exists g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

A **binary operation** combines two elements, taken in order, into one result. Addition and multiplication of numbers are binary operations, and so is composition of functions.

Property	In words
closure	Combining two elements of G gives an element of G. The operation never leaves the set.
associativity	Three elements in a row can be bracketed either way.
identity	One element, e, changes nothing when combined with anything, on either side.
inverses	Every element has a partner in G that takes it back to e, on either side.

Points that are easy to read past:

- **A group is the pair.** The set alone is not a group, and neither is the operation. $(\mathbb{Z}, +)$ is a group and $(\mathbb{Z}, -)$ is not. They have the same set.
- **Both sides.** The identity must satisfy $e * g = g$ *and* $g * e = g$. An inverse must work on both sides too.
- **The order of the quantifiers.** Property (3) is $\exists e \, \forall g$: a single e that works for every g. Property (4) is $\forall g \, \exists g^{-1}$: each g has its own inverse (quantified-statements[7]).
- **g^{-1} is notation for "the inverse of g in this group".** In $(\mathbb{R}, +)$, $x^{-1} = -x$. It is a reciprocal only when the operation is multiplication.
- **The inverse must be in G.** In $(\mathbb{Z} - \{0\}, \cdot)$ the equation $2 \cdot y = 1$ has the solution $\frac{1}{2}$, which is not in the set. So 2 has no inverse there.

Commutative and abelian

A binary operation $*$ on S is **commutative** if $a * b = b * a$ for all $a, b \in S$. A group is **abelian** if and only if its operation is commutative.

[7] courses/math1061/quantified-statements.pdf

Commutativity is **not** one of the four properties. A group may or may not have it.

abelian	$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} - \{0\}, \cdot)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_7 - \{[0]\}, \cdot)$
non-abelian	$(S_3, \circ)$: $f_2 \circ f_3 = f_6$ but $f_3 \circ f_2 = f_5$
	$(F, \circ)$, the functions $ax + b$ with $a \neq 0$
	(below): with $f(x) = 2x$ and $g(x) = x + 1$,
	$(f \circ g)(x) = 2x + 2$ but $(g \circ f)(x) = 2x + 1$

In a group that is not known to be abelian, **keep the order of every product**, and do the same thing on the same side of both sides of an equation. To show a group is not abelian, one pair with $a * b \neq b * a$ is enough (2026-09-24-definitions-and-examples-of-groups[8]).

Associativity is about brackets, not order

Associativity says $(g * h) * k = g * (h * k)$. The three elements stay in the same order, and only the bracketing changes. It is what allows $g * h * k$ to be written with no brackets at all. It says nothing about swapping elements, which is commutativity.

Subtraction on $\mathbb{Z}$ is an operation that is not associative: $(3 - 2) - 1 = 0$ but $3 - (2 - 1) = 2$. The figure sets it beside addition, which is.

Operation	Associative	Commutative
$+$ and $\cdot$ on numbers	yes	yes
$\circ$ on functions	yes	no
$-$ on $\mathbb{Z}$	no	no

Checking the four properties

Each property is a quantified statement, so each is proved in general and disproved with specific elements.

Property	To show it holds	To show it fails
closure	Take arbitrary $g, h \in G$ and show $g * h \in G$.	Two elements of G whose result is outside G.

[8] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

Property	To show it holds	To show it fails
associativity	Usually inherited: the operation is built from addition or multiplication of numbers, or is composition of functions. Otherwise compute both bracketings for arbitrary g, h, k.	Three elements whose two bracketings differ.
identity	Name e, check $e \in G$, and check $e * g = g$ and $g * e = g$ for arbitrary g.	Show that no element can do the job.
inverses	For arbitrary g, name g^{-1}, check it is in G, and check both products are e.	One element of G with no inverse in G.

Do identity before inverses, since inverses are defined in terms of e. When e or g^{-1} is not obvious, **solve for it**: write down the equation it has to satisfy and solve.

Worked: an unfamiliar operation

From practice-problems[9], Q2. Let G be the set of odd integers, with $x \star y = x + y - 1$.

- **Closure.** If x, y are odd then $x + y$ is even, so $x + y - 1$ is odd.
- **Associativity.** $(x \star y) \star z = (x + y - 1) + z - 1 = x + y + z - 2$, and $x \star (y \star z) = x + (y + z - 1) - 1 = x + y + z - 2$.
- **Identity.** Solve $x \star e = x$: $x + e - 1 = x$ gives $e = 1$, which is odd. Check the other side: $1 \star x = 1 + x - 1 = x$.
- **Inverses.** Solve $x \star y = 1$: $x + y - 1 = 1$ gives $y = 2 - x$, which is odd when x is. So $x^{-1} = 2 - x$.

It is also commutative, since $x + y - 1 = y + x - 1$, so $(G, \star)$ is an abelian group. The identity is 1, not 0, and the inverse of x is $2 - x$, not $-x$. They are whatever the operation makes them.

Eight candidates

Which of these eight pairs are groups (2026-09-24-definitions-and-examples-of-groups[10])? All eight against all four properties:

[9] courses/math1061/practice-problems.pdf
[10] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

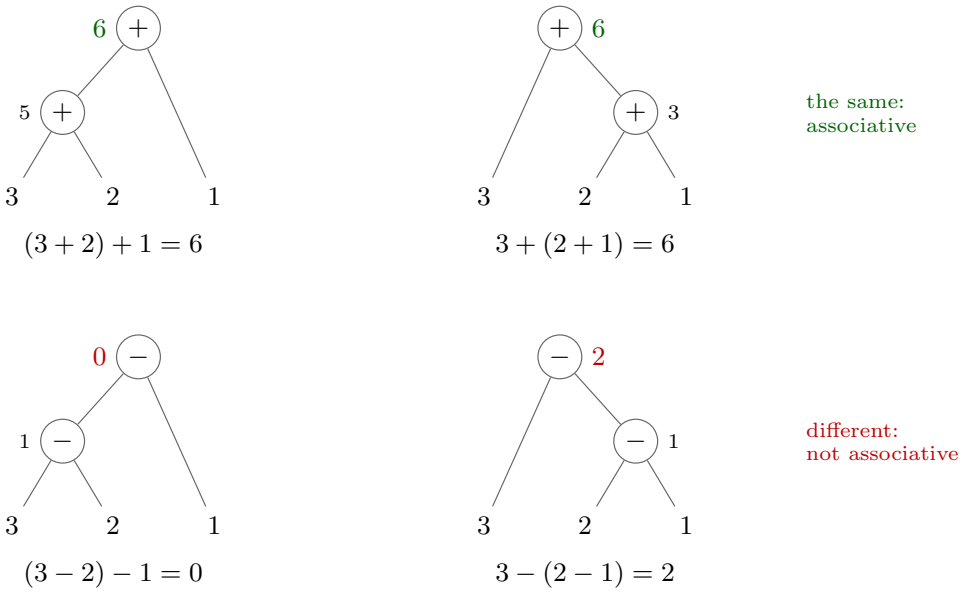


Figure 1: The two ways of bracketing three elements, drawn as trees: the lower operation is done first, and its result feeds the upper one. Top row, addition: both bracketings of $3+2+1$ give 6. Addition is associative, so the brackets can be dropped. Bottom row, subtraction: $(3-2)-1=0$ and $3-(2-1)=2$. The same three numbers in the same order give different answers, so subtraction is not associative and $(\mathbb{Z},-)$ is not a group.

	Closure	Associative	Identity	Inverses	Group?
$(\mathbb{Z}, +)$	✓	✓	0	$-x$	**yes**
$(\mathbb{Z} - \{0\}, \cdot)$	✓	✓	1	$\times$ 2 has none	**no**
$(\mathbb{Z}, -)$	✓	$\times$ $(3-2)-1 \neq 3-(2-1)$	$\times$	—	**no**
$(\mathbb{Z}_3, +)$	✓	✓	$[0]$	$[-a]$	**yes**
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	✓	✓	$[1]$	✓	**yes**
$(\mathbb{R}, +)$	✓	✓	0	$-x$	**yes**
$(\mathbb{R}, \cdot)$	✓	✓	1	$\times$ 0 has none	**no**
$(\mathbb{R} - \{0\}, \cdot)$	✓	✓	1	$\frac{1}{x}$	**yes**

Some of the entries need a word:

- $(\mathbb{Z} - \{0\}, \cdot)$**.** Closed, associative, identity 1. Only 1 and -1 have inverses in the set.
- $(\mathbb{Z}, -)$**.** As well as failing associativity it has no identity. $g - e = g$ forces $e = 0$, but $0 - g = -g$, which is not g unless $g = 0$. So 0 works on the right only.
- $(\mathbb{R}, \cdot)$ **and** $(\mathbb{R} - \{0\}, \cdot)$**.** The only obstacle is 0, since $0 \cdot y = 1$ has no solution. Removing it leaves a set that is still closed, because a product of non-zero reals is non-zero.
- $(\mathbb{Z}_5 - \{[0]\}, \cdot)$**.** Its table is Q4 of practice-problems[11]: $[1]^{-1} = [1]$, $[2]^{-1} = [3]$, $[3]^{-1} = [2]$, $[4]^{-1} = [4]$.

Removing elements can also break closure. $\mathbb{Z}_9 - \{[0]\}$ is not a group under multiplication, because $[3] \cdot [3] = [0]$ is not in the set (the same practice set, Q1, which writes the classes without brackets). See integers-modulo-n[12].

A group of functions: $ax + b$

Let F be the set of all functions $f(x) = ax + b$ with $a \in \mathbb{R} - \{0\}$ and $b \in \mathbb{R}$. Under composition, $(F, \circ)$ is a group (2026-10-06-elementary-properties-of-groups[13]). Every check works the same way: compose, collect into the form (number) x + (number), and read off the coefficients.

Property	For $f(x) = ax + b$ and $g(x) = cx + d$
closure	$(f \circ g)(x) = (ac)\,x + (ad + b)$, and $ac \neq 0$ because $a, c \neq 0$
associativity	composition of functions is always associative (above)

[11] courses/math1061/practice-problems.pdf
[12] courses/math1061/integers-modulo-n.pdf
[13] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

Property	For $f(x) = ax + b$ and $g(x) = cx + d$
identity	$I(x) = x$, found by solving $I \circ f = f$ for the coefficients of I
inverses	$f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$, found by solving $f \circ g = I$ for c and d, then checked in the other order

The condition $a \neq 0$ is what keeps the inverses: a constant function $0x + b$ sends everything to b, and nothing undoes that. It is also a second non-abelian group, after S_3, since $f \circ g$ and $g \circ f$ have constants $ad + b$ and $cb + d$, which usually differ.

Why these four: solving equations

Solving $2x = 4$ means applying an inverse to both sides:

$$2x = 4, \qquad 2^{-1} \cdot 2x = 2^{-1} \cdot 4, \qquad x = 2.$$

The same steps solve $a * x = b$ in any group, and each step uses one property:

$$\begin{aligned} a * x &= b \\ a^{-1} * (a * x) &= a^{-1} * b && a^{-1} \text{ exists, by inverses} \\ (a^{-1} * a) * x &= a^{-1} * b && \text{by associativity} \\ e * x &= a^{-1} * b && \text{by inverses} \\ x &= a^{-1} * b && \text{by identity} \end{aligned}$$

The working shows that a solution can only be $a^{-1} * b$, and closure says that element is in G. It is a solution: $a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$. So in a group every equation $a * x = b$ has exactly one solution.

Two consequences:

- **Cancellation.** If $a * b = a * c$ then $b = c$: apply a^{-1} on the left of both sides. It is why a Cayley table has no repeats in a row (cayley-tables[14], proved in 2026-09-24-definitions-and-examples-of-groups[15]).
- **Sides matter.** a^{-1} went on the *left* of both sides because a was on the left. For $x * a = b$ it goes on the right, giving $x = b * a^{-1}$. In a non-abelian group $a^{-1} * b$ and $b * a^{-1}$ can differ.

[14] courses/math1061/cayley-tables.pdf
[15] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

Without inverses an equation can have no solution. In $(\mathbb{Z} - \{0\}, \cdot)$, $2x = 3$ has none, because 2 has no inverse.

Elementary properties

A handful of facts follow from the four properties alone, so they hold in every group. They are what justify writing *the* identity and *the* inverse.

The identity is unique. Suppose e and e' are both identities. Then

$$e = e * e' = e',$$

the first step because e' is an identity and the second because e is.

Each element has exactly one inverse. Suppose h and k are both inverses of g. Then

$$h = h * e = h * (g * k) = (h * g) * k = e * k = k,$$

using identity, k an inverse, associativity, h an inverse, and identity. So to show that some x *is* g^{-1}, it is enough to show $g * x = x * g = e$.

The inverse of an inverse. $g * g^{-1} = g^{-1} * g = e$ says, read the other way round, that g is an inverse of g^{-1}. By uniqueness,

$$(g^{-1})^{-1} = g.$$

Equivalently, if $g^{-1} = h$ then $h^{-1} = g$. Inverses come in pairs, or an element is its own inverse, as the three swaps in S_3 are.

The inverse of a product reverses the order.

$$(g * h)^{-1} = h^{-1} * g^{-1}.$$

Check both products, using associativity to regroup:

$$(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * e * g^{-1} = g * g^{-1} = e,$$

$$(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * e * h = h^{-1} * h = e.$$

By uniqueness, $h^{-1} * g^{-1}$ is the inverse of $g * h$. The last thing done is the first thing undone, as with putting on socks and then shoes.

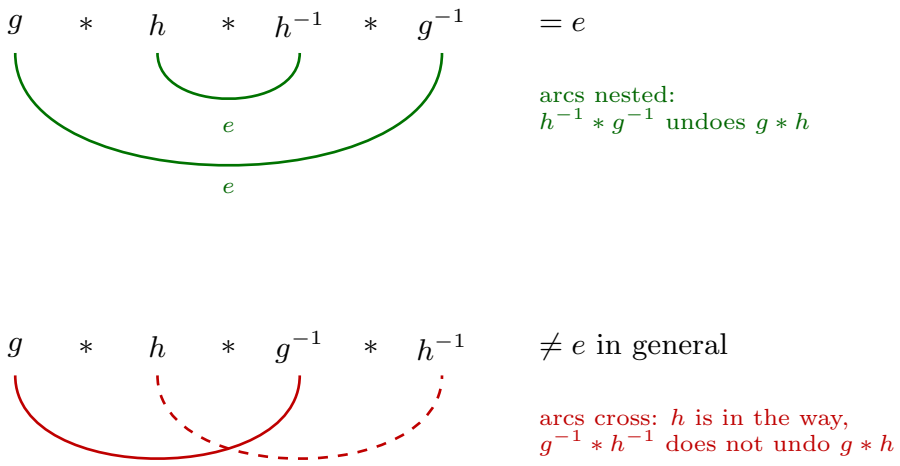


Figure 2: Why the inverse of $g * h$ is $h^{-1} * g^{-1}$ and not $g^{-1} * h^{-1}$. Top: in $g * h * h^{-1} * g^{-1}$ each element sits next to its inverse once the inner pair is gone. The inner arc, $h * h^{-1} = e$, cancels first, and that brings g next to g^{-1}, so the whole product is e. The arcs are nested. Bottom: in $g * h * g^{-1} * h^{-1}$ the arcs cross. h sits between g and g^{-1}, and nothing cancels unless h and g^{-1} can be swapped, which needs the group to be abelian.

A check in S_3 (symmetric-group[16]). $f_2 \circ f_3 = f_6$, so $(f_2 \circ f_3)^{-1} = f_6^{-1} = f_5$. The reversed product of the inverses is $f_3^{-1} \circ f_2^{-1} = f_3 \circ f_2 = f_5$, which agrees. The unreversed one is $f_2^{-1} \circ f_3^{-1} = f_2 \circ f_3 = f_6$, which does not. In an abelian group the order makes no difference, and $(g * h)^{-1} = g^{-1} * h^{-1}$ is also true.

A check with functions. In $(F, \circ)$, take $f(x) = 2x$ and $g(x) = x + 1$, so $f^{-1}(x) = \frac{1}{2}x$ and $g^{-1}(x) = x - 1$. Then $(f \circ g)(x) = 2x + 2$, whose inverse is $\frac{1}{2}x - 1$. Reversed: $(g^{-1} \circ f^{-1})(x) = \frac{1}{2}x - 1$, the same. Unreversed: $(f^{-1} \circ g^{-1})(x) = \frac{1}{2}(x - 1) = \frac{1}{2}x - \frac{1}{2}$, which is not.

Cancellation. If $a * b = a * c$ then $b = c$, and if $b * a = c * a$ then $b = c$. Proved above by applying a^{-1} on the same side as a.

Powers. For every $g \in G$ and $i, j \in \mathbb{Z}$, $g^i * g^j = g^{i+j}$ and $(g^i)^{-1} = g^{-i}$, where $g^0 = e$ and a negative power is a power of g^{-1} (subgroups-and-cyclic-groups[17]).

The inverse facts are Q2 of practice-problems[18].

Common mistakes

- **Leaving out the operation.** "$\mathbb{Z}$ is a group" is incomplete. $(\mathbb{Z}, +)$ is, $(\mathbb{Z}, -)$ and $(\mathbb{Z} - \{0\}, \cdot)$ are not.
- **Assuming closure.** It is the property most often taken for granted, and the one that fails for $\mathbb{Z}_9 - \{[0]\}$.
- **Checking the identity or an inverse on one side.**
- **Accepting an inverse that is outside the set.**
- **Assuming the operation is commutative.** Swapping $g * h$ for $h * g$, or applying a^{-1} on the left of one side and the right of the other, needs the group to be abelian.
- **Confusing associative with commutative.**
- **Reading g^{-1} as $\frac{1}{g}$** whatever the operation.
- **$(g * h)^{-1} = g^{-1} * h^{-1}$.** The inverse of a product reverses the order: $(g * h)^{-1} = h^{-1} * g^{-1}$. The two agree only when g^{-1} and h^{-1} commute.
- **A disproof without elements.** "Subtraction isn't associative" needs $(3 - 2) - 1 = 0$ and $3 - (2 - 1) = 2$ beside it.

See also

- cayley-tables[19] — a finite group as a table, and what can be read off it
- integers-modulo-n[20] — $\mathbb{Z}_n$ under addition, and $\mathbb{Z}_n - \{[0]\}$ under multiplication

[16] courses/math1061/symmetric-group.pdf
[17] courses/math1061/subgroups-and-cyclic-groups.pdf
[18] courses/math1061/practice-problems.pdf
[19] courses/math1061/cayley-tables.pdf
[20] courses/math1061/integers-modulo-n.pdf

- symmetric-group[21] — the group of bijections of $\{1, \dots, n\}$, the course's non-abelian example
- subgroups-and-cyclic-groups[22] — subgroups, powers of an element, cyclic subgroups and cyclic groups
- fields[23] — two abelian groups on one set, under $+$ and under $\cdot$, joined by the distributive laws
- composition-of-functions[24] — the operation of S_n and of the group of functions $ax + b$
- quantified-statements[25] — the two orders of quantifiers in the identity and inverse properties
- proof-techniques[26] — direct proof and counterexample, the methods the checks use
- 2026-09-24-definitions-and-examples-of-groups[27] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[28] — Lecture 27
- practice-problems[29] — §33, with full worked solutions · practice-problems[30] — §34

[21] courses/math1061/symmetric-group.pdf
[22] courses/math1061/subgroups-and-cyclic-groups.pdf
[23] courses/math1061/fields.pdf
[24] courses/math1061/composition-of-functions.pdf
[25] courses/math1061/quantified-statements.pdf
[26] courses/math1061/proof-techniques.pdf
[27] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[28] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[29] courses/math1061/practice-problems.pdf
[30] courses/math1061/practice-problems.pdf