Lecture 27 — Elementary Properties of Groups

Table of contents

Goals . . . 2
A group inside a group . . . 2
Worked: the functions $ax + b$ form a group . . . 2
Subgroups . . . 6
Worked: is $\mathbb{Z}$ a subgroup of $(\mathbb{R}, +)$? . . . 6
Worked: is $\mathbb{R} - \{0\}$ a subgroup of $(\mathbb{R}, +)$? . . . 7
Powers of an element . . . 7
Worked: $[3]^4$ and $[3]^{-4}$ in $\mathbb{Z}_7 - \{[0]\}$ . . . 8
Cyclic subgroups . . . 9
Worked: $\langle 3 \rangle$ in $\mathbb{Z}_{11} - \{[0]\}$ . . . 9
Worked: all the cyclic subgroups of $(\mathbb{Z}_8, +)$ . . . 11
Cyclic groups . . . 12
Worked: which of these groups are cyclic? . . . 12
Worked: $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic . . . 13
See also . . . 14

One more group checked from the definition, the functions $ax + b$ under composition, and then three new ideas: a **subgroup**, a group sitting inside another under the same operation; **powers** of an element, including zero and negative powers; and the **cyclic subgroup** an element generates, which leads to **cyclic groups**. Pre-work: Video 034 (Elementary Properties of Groups). Subgroups, powers, cyclic subgroups and cyclic groups are collected in subgroups-and-cyclic-groups[1], the definition of a group and the rules for inverses in groups[2], and the classes $[a]$ in integers-modulo-n[3]. How a subgroup shows up in a table is in cayley-tables[4]. The cyclic subgroups of $\mathbb{Z}_8$ and cyclic groups are also worked in 2026-10-08-definitions-and-examples-of-fields[5].

[1] courses/math1061/subgroups-and-cyclic-groups.pdf
[2] courses/math1061/groups.pdf
[3] courses/math1061/integers-modulo-n.pdf
[4] courses/math1061/cayley-tables.pdf
[5] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

Goals

1. Become more familiar with **groups**.
2. Understand **subgroups** and other elementary properties of groups.
3. Learn how to work with **powers** of elements in groups and to generate **cyclic subgroups**.

A question to keep in mind:

- **What does it mean for a group $(G, *)$ to be cyclic?** That every element of G is a power of one single element. The definition is below, after the powers it needs.

A group inside a group

Here is the Cayley table of $(\mathbb{Z}_6, +)$ with its elements listed in an unusual order, the even classes $[0], [2], [4]$ first and then the odd ones $[1], [3], [5]$.

So $\{[0], [2], [4]\}$ is a group under the same operation as $\mathbb{Z}_6$, made of some of its elements. That is what a subgroup is. It is also exactly the set of multiples of $[2]$, $\{[2], [2]+[2], [2]+[2]+[2]\} = \{[2], [4], [0]\}$, which makes it the cyclic subgroup generated by $[2]$. Listing a subgroup's elements first, to make it a block, works for any subgroup of any finite group (cayley-tables[6]).

Worked: the functions $ax + b$ form a group

> Show that $(F, \circ)$ is a group, where F is the set of all functions of the form $f(x) = ax + b$ where $a \in \mathbb{R} - \{0\}$ and $b \in \mathbb{R}$, and $\circ$ is function composition.

The four properties to check, numbered as in groups[7]:

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

Here G is F, $*$ is $\circ$, and the identity will turn out to be $I(x) = x$.

An element of F is a straight-line function with a non-zero slope, and it is pinned down by two numbers: the coefficient $a \neq 0$ and the constant b. Every check below comes down to the same move. Work out a composite, collect it into the form (number) x + (number), and see whether the coefficient of x is non-zero.

[6] courses/math1061/cayley-tables.pdf
[7] courses/math1061/groups.pdf

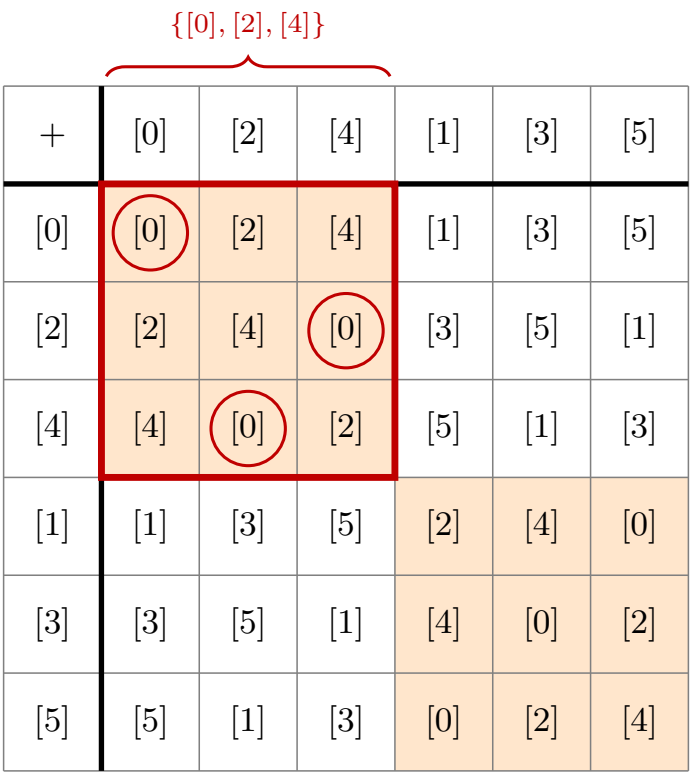


Figure 1: The table of $(\mathbb{Z}_6, +)$ with the even classes listed first. The top-left block, outlined, is a complete table on its own: its headings are $[0], [2], [4]$ and its body uses only $[0], [2], [4]$. So that set is closed under $+$, it contains the identity $[0]$, and the rings show each element's inverse inside it: $[0] + [0] = [0]$ and $[2] + [4] = [4] + [2] = [0]$. It is a group in its own right, a subgroup of $\mathbb{Z}_6$. Shaded cells hold even classes. The bottom-right block is also all even, but its headings are odd, so it is not the table of anything: an odd plus an odd is even.

Throughout, let

$$f(x) = ax + b, \qquad g(x) = cx + d, \qquad h(x) = mx + n,$$

where $a, b, c, d, m, n \in \mathbb{R}$ and $a, c, m \neq 0$.

(1) Closure. Show that if $f, g \in F$ then $f \circ g \in F$.

$$\begin{aligned}(f \circ g)(x) &= f(cx + d) \\ &= a(cx + d) + b \\ &= (ac)\,x + (ad + b).\end{aligned}$$

This is $Ax + B$ with $A = ac$ and $B = ad + b$. Since $a, b, c, d \in \mathbb{R}$, both ac and $ad + b$ are in $\mathbb{R}$. Since $a \neq 0$ and $c \neq 0$, $ac \neq 0$. So $f \circ g \in F$, and F is closed. ✓

(2) Associativity. Show that $(f \circ g) \circ h = f \circ (g \circ h)$. Let $y = h(x) = mx + n$. Then, using the closure working,

$$\begin{aligned}((f \circ g) \circ h)(x) &= (f \circ g)(y) = f(cy + d) \\ &= a(cy + d) + b = (ac)\,y + (ad + b) \\ &= (ac)(mx + n) + (ad + b) \\ &= (acm)\,x + (acn + ad + b),\end{aligned}$$

and

$$\begin{aligned}(f \circ (g \circ h))(x) &= f(g(mx + n)) = f(c(mx + n) + d) \\ &= f((cm)\,x + (cn + d)) \\ &= a((cm)\,x + cn + d) + b \\ &= (acm)\,x + (acn + ad + b).\end{aligned}$$

The two agree for every x, so $(f \circ g) \circ h = f \circ (g \circ h)$. ✓ Composition of functions is always associative (groups[8]), so this could have been quoted; the algebra confirms it for this family.

(3) Identity. Show that there is an $I \in F$ with $f = I \circ f = f \circ I$ for all $f \in F$. Suppose $I(x) = ix + j$ is in F and works, and find i and j. For $f = I \circ f$:

[8] courses/math1061/groups.pdf

$$\begin{aligned} f(x) &= (I \circ f)(x) \\ ax + b &= I(ax + b) \\ &= i(ax + b) + j \\ &= (ia)\, x + (ib + j). \end{aligned}$$

Two straight-line functions are equal for every x exactly when their coefficients match, so

$$\begin{cases} a = ia & \Rightarrow\ i = 1 \quad (\text{since } a \neq 0), \\ b = ib + j & \Rightarrow\ b = b + j \ \Rightarrow\ j = 0. \end{cases}$$

So $I(x) = 1x + 0 = x$. It is in F, because its coefficient 1 is non-zero, and it satisfies $f = I \circ f$ for all $f \in F$. The other side: $(f \circ I)(x) = f(I(x)) = f(x)$, so $f \circ I = f$. F **has identity** $I(x) = x$**.** ✓

(4) Inverses. Show that for every $f \in F$ there is an $f^{-1} \in F$ with $f \circ f^{-1} = f^{-1} \circ f = I$. Let $f(x) = ax + b$ with $a \neq 0$, and suppose $g(x) = cx + d$, with $c \neq 0$, satisfies $f \circ g = I$. Then

$$\begin{aligned} I(x) &= (f \circ g)(x) \\ x &= f(cx + d) = a(cx + d) + b \\ &= (ac)\, x + (ad + b). \end{aligned}$$

Equating coefficients, with $x = 1x + 0$ on the left:

$$\begin{cases} 1 = ac & \Rightarrow\ c = \dfrac{1}{a} \in \mathbb{R} - \{0\} \quad (\text{since } a \neq 0 \text{ and } a \in \mathbb{R}), \\ 0 = ad + b & \Rightarrow\ d = -\dfrac{b}{a} \in \mathbb{R} \qquad\quad (\text{since } a \neq 0 \text{ and } a, b \in \mathbb{R}). \end{cases}$$

So $g(x) = \frac{1}{a}x - \frac{b}{a}$, which is in F. It was found from $f \circ g = I$ alone, so check the other order:

$$(g \circ f)(x) = g(ax + b) = \frac{1}{a}(ax + b) - \frac{b}{a} = x + \frac{b}{a} - \frac{b}{a} = x = I(x).$$

So $g \circ f = f \circ g = I$, and $g = f^{-1}$: **the inverse of** $f(x) = ax + b$ **is** $f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$**.** ✓ For instance $f(x) = 2x + 6$ has $f^{-1}(x) = \frac{1}{2}x - 3$. "Double, then add 6" is undone by "subtract 6, then halve".

All four properties hold, so $(F, \circ)$ **is a group.**

Two remarks:

- **Why $a \neq 0$.** With $a = 0$ the function $f(x) = b$ is constant. It sends everything to b, so nothing composed with it can give back x, and it has no inverse. Leaving out $a = 0$ is what makes F a group, in the same way that leaving out 0 turns $(\mathbb{R}, \cdot)$ into the group $(\mathbb{R} - \{0\}, \cdot)$.
- **F is not abelian.** In general $f \circ g = (ac)\,x + (ad + b)$ and $g \circ f = (ca)\,x + (cb + d)$ have different constants. With $f(x) = 2x$ and $g(x) = x + 1$, $(f \circ g)(x) = 2x + 2$ but $(g \circ f)(x) = 2x + 1$. So, like S_3 (symmetric-group[9]), this is a group in which the order of a composition matters.

Subgroups

> **Definition.** If $(G, *)$ is a group and $H \subseteq G$, then H is a **subgroup** of G if $(H, *)$ is itself a group.

The operation is the same one. To check that $(H, *)$ is a subgroup of $(G, *)$, check three properties:

- **closure**: for all $g, h \in H$, $g * h \in H$;
- **identity**: the identity is in H;
- **inverses**: for every $h \in H$, its inverse is in H.

Associativity is not on the list, because H inherits it. $(g*h)*k = g*(h*k)$ holds for all $g, h, k \in G$, so in particular it holds for all $g, h, k \in H$. G associative $\Rightarrow$ H associative under $*$. The other three can fail, because each one asks for an element to be *in* H. More on subgroups, and why the identity of H has to be the identity of G, is in subgroups-and-cyclic-groups[10].

Worked: is $\mathbb{Z}$ a subgroup of $(\mathbb{R}, +)$?

> True or false: $\mathbb{Z}$ is a subgroup of $(\mathbb{R}, +)$.

True. To prove it, show that the three properties hold for all elements. $\mathbb{Z} \subseteq \mathbb{R}$. Let $a, b \in \mathbb{Z}$.

- **Closure ✓.** $a + b \in \mathbb{Z}$, so $\mathbb{Z}$ is closed under $+$.
- **Identity ✓.** $0 \in \mathbb{Z}$, since $a + 0 = 0 + a = a$.
- **Inverses ✓.** $-a \in \mathbb{Z}$, and $a + (-a) = (-a) + a = 0$.

Associativity comes free from $(\mathbb{R}, +)$, so $\mathbb{Z}$ is a subgroup of $(\mathbb{R}, +)$.

[9] courses/math1061/symmetric-group.pdf
[10] courses/math1061/subgroups-and-cyclic-groups.pdf

Worked: is $\mathbb{R} - \{0\}$ a subgroup of $(\mathbb{R}, +)$?

True or false: $\mathbb{R} - \{0\}$ is a subgroup of $(\mathbb{R}, +)$.

False. To disprove it, one property failing for specific elements is enough: a counterexample to one property.

- **Closure** $\times$. Let $a \in \mathbb{R} - \{0\}$. Then $-a \in \mathbb{R} - \{0\}$ as well, but $a + (-a) = 0 \notin \mathbb{R} - \{0\}$. For example $1 + (-1) = 0$. So the set is not closed under $+$.
- **Identity** $\times$. The identity of $(\mathbb{R}, +)$ is 0, and it has been removed. No other element could stand in for it, since $e + a = a$ forces $e = 0$.
- **Inverses.** There is nothing to check against: an inverse is defined as an element that combines with a to give the identity, and there is no identity.

The same set *is* a group under multiplication, $(\mathbb{R} - \{0\}, \cdot)$ (groups[11]). But a subgroup must use the operation of the group it sits in, and under $+$ it fails.

Powers of an element

If $(G, *)$ is a group and $a \in G$, then a^i is defined for each $i \in \mathbb{Z}$ as follows:

$a^0 = e$, where e is the identity of G;

$a^i = \underbrace{a * a * \cdots * a}_{i \text{ times}}$ for each $i \in \mathbb{Z}^+$;

$a^{-i} = \underbrace{a^{-1} * a^{-1} * \cdots * a^{-1}}_{i \text{ times}}$ for each $i \in \mathbb{Z}^+$.

So $a^1 = a$, $a^2 = a * a$, $a^3 = a * a * a$, and so on. A negative power is a power of the inverse: a^{-1}, one copy of the inverse, is the inverse of a under $*$, exactly as before, and $a^{-2} = a^{-1} * a^{-1}$.

The power notation is used for any operation $*$, even if that operation is addition. Be careful with it.

- In $(\mathbb{Z}_{12}, +)$, $3^2 = 3 + 3 = 6$. It is not 9.
- In $(\mathbb{Z}, +)$, $a^2 = a + a$, and $a^{-1} = -a$, because $a^{-1} + a = 0$.

Two laws. For all $g \in G$:

$$g^i * g^j = g^{i+j}, \qquad \text{because} \qquad \underbrace{g * g * \cdots * g}_{i \text{ times}} * \underbrace{g * g * \cdots * g}_{j \text{ times}} \text{ is } i + j \text{ copies of } g,$$

and

[11] courses/math1061/groups.pdf

$$\underbrace{g * g * \cdots * g}_{i \text{ times}} * \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{i \text{ times}} = e,$$

because the g and the g^{-1} that meet in the middle combine to e, which drops out, and then the next pair meet, until nothing is left. So

$$(g^i)^{-1} = g^{-i}, \qquad g^i * g^{-i} = g^{i-i} = g^0 = e, \qquad g^{-i} * g^i = g^{-i+i} = g^0 = e.$$

The powers of a group element follow the same exponent rules as powers of a number. The laws for exponents of mixed sign, and a picture of the powers as a line or a loop, are in subgroups-and-cyclic-groups[12].

Worked: $[3]^4$ and $[3]^{-4}$ in $\mathbb{Z}_7 - \{[0]\}$

Calculate $[3]^4$ and $[3]^{-4}$ in the group $(\mathbb{Z}_7 - \{[0]\}, \cdot)$.

Here $[3] = \{a \in \mathbb{Z} : a \equiv 3 \pmod 7\}$, the operation is multiplication of classes, and the identity is $[1]$.

$[3]^4$. Multiply, reducing mod 7 as soon as a product passes 6:

$$[3]^4 = [3] \cdot [3] \cdot [3] \cdot [3] = [9] \cdot [9] = [2] \cdot [2] = [\mathbf{4}].$$

$[3]^{-4}$. By definition $[3]^{-4} = ([3]^{-1})^4$, and by the second law it is also $([3]^4)^{-1}$. The second is quicker here, since $[3]^4$ is already known:

$$[3]^{-4} = ([3]^{-1})^4 = ([3]^4)^{-1} = [4]^{-1} = [\mathbf{2}],$$

because $[4] \cdot [2] = [8] = [1]$, that is, $4 \cdot 2 \equiv 1 \pmod 7$.

Check by the other route. $[3]^{-1} = [5]$, since $[3] \cdot [5] = [15] = [1]$. Then $[3]^{-4} = [5]^4 = [25] \cdot [25] = [4] \cdot [4] = [16] = [2]$. The same. And $[3]^4 \cdot [3]^{-4} = [4] \cdot [2] = [1] = [3]^0$, as the first law says it must be. Both inverses can also be read off the table of this group (2026-09-24-definitions-and-examples-of-groups[13]).

[12] courses/math1061/subgroups-and-cyclic-groups.pdf
[13] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

Cyclic subgroups

If $(G, *)$ is a group and $a \in G$, then

$$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}$$

is a subgroup of G, and is called the **cyclic subgroup of G generated by a.**

$\langle a \rangle$ is every power of a: positive, zero and negative. It is what any subgroup S containing a is forced to contain:

- $a \in S$, so by closure $a^2, a^3, a^4, ... \in S$;
- by identity $a^0 = e \in S$, and by inverses $a^{-1} \in S$, so by closure again $a^{-2}, a^{-3}, a^{-4}, ... \in S$.

And the powers are already a subgroup, by the two laws: closure from $a^i * a^j = a^{i+j}$, the identity a^0, inverses $(a^i)^{-1} = a^{-i}$. So $\langle a \rangle$ is the smallest subgroup that contains a.

In a finite group, list the positive powers $a^1, a^2, a^3, ...$ until the list comes back to where it started. After that it only repeats, and the negative powers turn out to be in the list already (subgroups-and-cyclic-groups[14]).

Worked: $\langle 3 \rangle$ in $\mathbb{Z}_{11} - \{[0]\}$

Determine $\langle 3 \rangle$ in the group $(\mathbb{Z}_{11} - \{[0]\}, \cdot)$.

Each power is the previous one times [3], reduced mod 11:

$$\begin{aligned}
[3]^1 &= [3] \\
[3]^2 &= [3] \cdot [3] = [9] \\
[3]^3 &= [3]^2 \cdot [3] = [9] \cdot [3] = [27] = [22 + 5] = [5] \\
[3]^4 &= [3]^3 \cdot [3] = [5] \cdot [3] = [15] = [11 + 4] = [4] \\
[3]^5 &= [3]^4 \cdot [3] = [4] \cdot [3] = [12] = [1] \\
[3]^6 &= [3]^5 \cdot [3] = [1] \cdot [3] = [3]
\end{aligned}$$

$[3]^6$ is back to the start, so every element of $\langle 3 \rangle$ has been found: $[3]^7 = [9]$, $[3]^8 = [5]$, and so on round again. Once it is clear which group is meant, the square brackets are optional:

$$\langle 3 \rangle = \{3, 3^2, 3^3, ...\} = \{3, 9, 5, 4, 1\}.$$

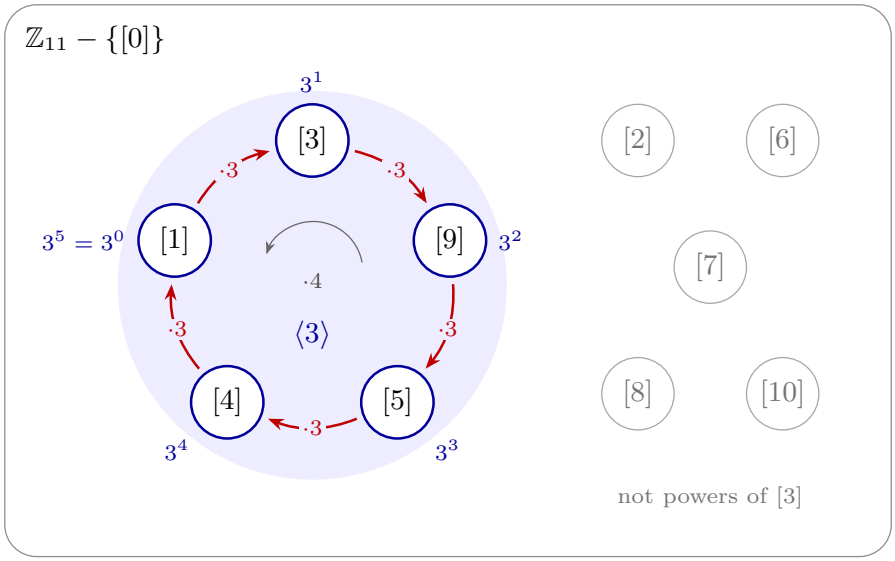


Figure 2: The powers of [3] in $\mathbb{Z}_{11} - [0]$. Each arrow multiplies by [3]. Starting from [3] the powers run $[3], [9], [5], [4], [1]$, and since $[3]^5 = [1]$ the next step is back at [3], so the powers go round a loop of five and $\langle 3 \rangle = 1, 3, 4, 5, 9$. Going round backwards is multiplying by $[3]^{-1} = [4]$, which gives the negative powers and stays on the same loop. The other five elements of the group are not powers of [3], so $\langle 3 \rangle$ is a subgroup, not the whole group.

The negative powers add nothing. $[3]^5 = [1]$ gives $[3]^4 \cdot [3] = [1]$, so $[3]^{-1} = [3]^4 = [4]$ (check: $[3] \cdot [4] = [12] = [1]$). Multiplying by $[3]^{-1}$ walks round the same loop backwards, so $[3]^{-1}, [3]^{-2}, \ldots$ are $[4], [5], [9], [3], [1], \ldots$, all already listed.

$\langle 3 \rangle$ has 5 of the group's 10 elements, so 3 does not generate the whole group. Another element does: the powers of 2 are all ten elements (practice-problems[15], Q4).

Worked: all the cyclic subgroups of $(\mathbb{Z}_8, +)$

Determine all the cyclic subgroups of $(\mathbb{Z}_8, +)$.

$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, writing the classes without brackets, and any representative names its class, so $9 = 1$ and $8 = 0$. The operation is $+$, so a power is a repeated sum: $2^3 = 2+2+2 = 6$. One cyclic subgroup for each element, starting with the identity:

$$\begin{aligned}
\langle 0 \rangle &= \{0\} \\
\langle 1 \rangle &= \{1, 2, 3, 4, 5, 6, 7, 8 = 0\} = \mathbb{Z}_8 \\
\langle 2 \rangle &= \{2^n : n \in \mathbb{Z}\} = \{2^1, 2^2, 2^3, 2^4, \ldots\} = \{2, 4, 6, 0\} \\
\langle 3 \rangle &= \{3, 6, 9 = 1, 4, 7, 10 = 2, 5, 0\} = \mathbb{Z}_8 \\
\langle 4 \rangle &= \{4, 8 = 0\} = \{0, 4\}
\end{aligned}$$

Each list stops at 0, the identity, because the next power is back at the start. The last three need no more work, because $5 = -3$, $6 = -2$ and $7 = -1$ are inverses of elements already done:

$$\langle 5 \rangle = \langle 3^{-1} \rangle = \mathbb{Z}_8, \qquad \langle 6 \rangle = \langle 2^{-1} \rangle = \{0, 2, 4, 6\}, \qquad \langle 7 \rangle = \langle 1^{-1} \rangle = \mathbb{Z}_8.$$

Two rules were used:

- $\langle \textbf{identity} \rangle = \{\textbf{identity}\}$**.** Every power of e is e.
- $\langle a \rangle = \langle a^{-1} \rangle$**.** The powers of a^{-1} are $(a^{-1})^i = a^{-i}$, the powers of a in the opposite order, so they make the same set. Directly: $\langle 5 \rangle = \{5, 10 = 2, 15 = 7, 20 = 4, 25 = 1, 30 = 6, 35 = 3, 40 = 0\}$, which is $\langle 3 \rangle$ listed backwards.

So $(\mathbb{Z}_8, +)$ has eight elements but only **four different cyclic subgroups**, and each one sits inside the next:

$$\{0\} \subset \{0, 4\} \subset \{0, 2, 4, 6\} \subset \mathbb{Z}_8.$$

Four of the eight elements, $1, 3, 5, 7$, generate the whole of $\mathbb{Z}_8$. That makes $\mathbb{Z}_8$ a cyclic group.

[14] courses/math1061/subgroups-and-cyclic-groups.pdf
[15] courses/math1061/practice-problems.pdf

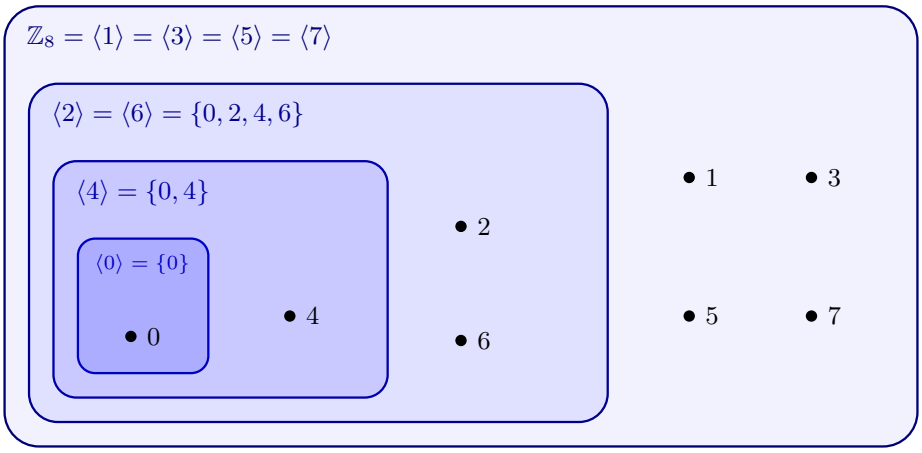


Figure 3: The four cyclic subgroups of $(\mathbb{Z}_8, +)$, each drawn inside the next. Every element generates exactly the smallest region it sits in: 0 generates only 0, 4 generates $0, 4$, 2 and 6 generate $0, 2, 4, 6$, and the four odd elements $1, 3, 5, 7$ each generate all of $\mathbb{Z}_8$. Elements that are inverses of each other, such as 2 and 6, always land in the same region, because $\langle a\rangle = \langle a^{-1}\rangle$.

Cyclic groups

The group $(G, *)$ is **cyclic** if there exists an $a \in G$ such that $\langle a\rangle = G$.

That answers the question in the goals: **a group is cyclic when every one of its elements is a power of a single element** a, called a **generator**. So far:

- $\mathbb{Z}_8$ is cyclic: $\langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \mathbb{Z}_8$.
- $\mathbb{Z}_6$ is cyclic, generated by $[1]$, since $[1], [1]+[1], \ldots$ runs through all six classes. Its subgroup $\{[0], [2], [4]\} = \langle [2]\rangle$, from the table above, is a cyclic subgroup that is not the whole group.
- $\mathbb{Z}_{11} - \{[0]\}$ is cyclic, generated by 2, even though 3 is not a generator. One generator is all it takes.

How to prove a group is cyclic, and how to prove it is not, is in subgroups-and-cyclic-groups[16].

Worked: which of these groups are cyclic?

Which of the following groups are cyclic? $(\mathbb{Z}_{10}, +)$, $(\mathbb{Z}_5 - \{[0]\}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$.

[16] courses/math1061/subgroups-and-cyclic-groups.pdf

Group	Cyclic?	Generated by
$(\mathbb{Z}_{10}, +)$	✓ yes	1
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	✓ yes	2
$(\mathbb{Z}, +)$	✓ yes	1
$(\mathbb{Q}, +)$	× no	nothing

$(\mathbb{Z}_{10}, +)$. $1^n = 1 + 1 + \cdots + 1 = n$, so the powers of 1 are $1, 2, \ldots, 9, 10 = 0$: every element. $\mathbb{Z}_{10} = \langle 1 \rangle$.

$(\mathbb{Z}_5 - \{[0]\}, \cdot)$. The set is $\{1, 2, 3, 4\}$. The identity is no use, since $\langle 1 \rangle = \{1\}$. Try 2: $2^1 = 2$, $2^2 = 4$, $2^3 = 8 = 3$, $2^4 = 16 = 1$. So $\langle 2 \rangle = \{2, 4, 3, 1\}$, the whole group. (3 is also a generator; 4 is not, since $\langle 4 \rangle = \{4, 1\}$.)

$(\mathbb{Z}, +)$. Here the negative powers are essential:

$$\langle 1 \rangle = \{1^n : n \in \mathbb{Z}\} = \{\ldots, 1^{-2}, 1^{-1}, 1^0, 1^1, 1^2, \ldots\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}.$$

The positive powers of 1 give only $1, 2, 3, \ldots$. The zero power is the identity 0, and $1^{-n} = (-1) + \cdots + (-1) = -n$ fills in the negatives.

$(\mathbb{Q}, +)$. Not cyclic. That means showing that *no* $a \in \mathbb{Q}$ generates it. In $(\mathbb{Q}, +)$ the powers of a are its integer multiples, so $\langle a \rangle = \{na : n \in \mathbb{Z}\}$.

- If $a = 0$, then $\langle a \rangle = \{0\} \neq \mathbb{Q}$.
- If $a = \frac{p}{q} \neq 0$, where $p, q \in \mathbb{Z}$ and $q \neq 0$, then $\frac{p}{2q} = \frac{a}{2} \in \mathbb{Q}$. But $\frac{p}{2q} = n \cdot \frac{p}{q}$ would need $n = \frac{1}{2}$, which is not an integer. So $\frac{p}{2q} \notin \left\langle \frac{p}{q} \right\rangle$, and $\langle a \rangle \neq \mathbb{Q}$.

Either way $\langle a \rangle \neq \mathbb{Q}$, so $(\mathbb{Q}, +)$ is not cyclic. The multiples of any one rational are evenly spaced with gaps, and half of it falls in the first gap. A picture is in subgroups-and-cyclic-groups[17].

Worked: $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic

> Consider the group $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ where $(a, b) + (c, d) = ((a+c) \bmod 2,\ (b+d) \bmod 3)$. Show that this group is cyclic.

The group has $2 \cdot 3 = 6$ elements, the pairs (a, b) with $a \in \{0, 1\}$ and $b \in \{0, 1, 2\}$, and its identity is $(0, 0)$. Take $(a, b) = (1, 1)$ and add it on each time:

[17] courses/math1061/subgroups-and-cyclic-groups.pdf

$$
\begin{aligned}
(1,1)^1 &= (1,1)\\
(1,1)^2 &= (1,1)+(1,1) = (2 \bmod 2,\ 2 \bmod 3) = (0,2)\\
(1,1)^3 &= (1,1)^2+(1,1) = (0,2)+(1,1) = (1,0)\\
(1,1)^4 &= (1,0)+(1,1) = (0,1)\\
(1,1)^5 &= (0,1)+(1,1) = (1,2)\\
(1,1)^6 &= (1,2)+(1,1) = (0,0)
\end{aligned}
$$

The six powers are six different elements, so they are the whole group: $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle$, and the group is cyclic. ■

It works because the first coordinate comes back to 0 every 2 steps and the second every 3 steps, and the two are back at 0 together for the first time at step 6. Not every element generates: $(0,1)$ gives only $\{(0,0),(0,1),(0,2)\}$ and $(1,0)$ only $\{(0,0),(1,0)\}$. These three are drawn in subgroups-and-cyclic-groups[18].

See also

- subgroups-and-cyclic-groups[19] — subgroups, powers and the power laws, $\langle a \rangle$, and cyclic groups, with more examples
- groups[20] — the four properties, and the elementary properties: unique identity and inverses, the inverse of a product
- cayley-tables[21] — reading a subgroup off a table by listing its elements first
- integers-modulo-n[22] — $\mathbb{Z}_n$ and $\mathbb{Z}_n - \{[0]\}$, the groups most of the examples live in
- composition-of-functions[23] · inverse-functions[24] — the operation and the inverses in the group $(F, \circ)$
- symmetric-group[25] — the cyclic subgroups of S_3, which is not cyclic
- 2026-09-24-definitions-and-examples-of-groups[26] — Lecture 26 · 2026-10-08-definitions-and-examples-of-fields[27] — Lecture 28
- practice-problems[28] — §34, with full worked solutions

[18] courses/math1061/subgroups-and-cyclic-groups.pdf
[19] courses/math1061/subgroups-and-cyclic-groups.pdf
[20] courses/math1061/groups.pdf
[21] courses/math1061/cayley-tables.pdf
[22] courses/math1061/integers-modulo-n.pdf
[23] courses/math1061/composition-of-functions.pdf
[24] courses/math1061/inverse-functions.pdf
[25] courses/math1061/symmetric-group.pdf
[26] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[27] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[28] courses/math1061/practice-problems.pdf