Subgroups and Cyclic Groups

Table of contents

Subgroups 1
Powers of an element 3
When the powers repeat 5
The cyclic subgroup generated by a 5
Cyclic groups 7
Common mistakes 10
See also 10

A **subgroup** is a group sitting inside another group under the same operation. The quickest way to build one is to take a single element and all of its **powers**, positive, zero and negative: that set is the **cyclic subgroup** the element generates. A group that is the cyclic subgroup of one of its own elements is a **cyclic group**. The definition of a group is in groups[1], and most of the examples live in integers-modulo-n[2]. First met in 2026-10-06-elementary-properties-of-groups[3], and cyclic groups are also worked in 2026-10-08-definitions-and-examples-of-fields[4].

Subgroups

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

To check that $(H, *)$ is a subgroup of $(G, *)$, check three of the four group properties:

[1] courses/math1061/groups.pdf
[2] courses/math1061/integers-modulo-n.pdf
[3] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[4] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

Property	To show it holds	To show it fails
closure	Take arbitrary $g, h \in H$ and show $g * h \in H$.	Two elements of H whose result is outside H.
identity	Show that the identity e of G is in H.	Show $e \notin H$.
inverses	Take arbitrary $h \in H$ and show its inverse in G is in H.	One element of H whose inverse is outside H.

Associativity is inherited. $(g * h) * k = g * (h * k)$ holds for all $g, h, k \in G$, and elements of H are elements of G, so it holds for all $g, h, k \in H$. Nothing new has to be checked. The other three properties are different: each one says some element must be *in the set*, and a smaller set can leave it out.

Points to watch:

- **The same operation.** $\mathbb{R} - \{0\}$ is a group under multiplication, but it is not a subgroup of $(\mathbb{R}, +)$: under $+$ it is not closed, since $1 + (-1) = 0$, and it has no identity (2026-10-06-elementary-properties-of-groups[5]).
- **The identity of H is the identity of G.** If some $f \in H$ worked as an identity for H, then $f * f = f = f * e$ in G, and cancelling f on the left (groups[6]) gives $f = e$. So the identity check is simply: **is $e \in H$?** It also makes sure H is not empty.
- **The inverse of h in H is its inverse in G**, for the same reason: inverses in a group are unique (groups[7]). So the inverses check is: **for each $h \in H$, is $h^{-1} \in H$?**

Every group has two subgroups for free: $\{e\}$, and G itself.

H	G	Subgroup?	Why
$\mathbb{Z}$	$(\mathbb{R}, +)$	**yes**	$a + b \in \mathbb{Z}$, $0 \in \mathbb{Z}$, $-a \in \mathbb{Z}$ (2026-10-06-elementary-properties-of-groups[8])
$\mathbb{R} - \{0\}$	$(\mathbb{R}, +)$	**no**	$1 + (-1) = 0 \notin H$, and 0, the identity, is missing
$\{3n : n \in \mathbb{Z}\}$	$(\mathbb{Z}, +)$	**yes**	$3a + 3b = 3(a + b)$, $0 = 3 \cdot 0$, $-3a = 3(-a)$

[5] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[6] courses/math1061/groups.pdf
[7] courses/math1061/groups.pdf
[8] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

H	G	Subgroup?	Why
$\{[0],[2],[4]\}$	$(\mathbb{Z}_6,+)$	**yes**	its block of the table uses only its own elements (cayley-tables[9])
$\{[0],[1]\}$	$(\mathbb{Z}_6,+)$	**no**	$[1]+[1]=[2]\notin H$

The multiples of 3 are Q1 of practice-problems[10], worked there in full.

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 $i\in\mathbb{Z}^+$.

A positive power combines a with itself; a negative power does the same with the inverse a^{-1}; and the zero power is the identity, the result of combining nothing. The definition agrees with itself at $i=1$: $a^1=a$, and a^{-1} is one copy of the inverse of a, which is what a^{-1} already meant.

The notation does not change with the operation, and in an additive group that takes care:

Group	a^2	a^3	a^0	a^{-1}
$(\mathbb{R}-\{0\},\cdot)$	$a\cdot a$	$a\cdot a\cdot a$	1	$\frac{1}{a}$
$(\mathbb{Z},+)$	$a+a=2a$	$3a$	0	$-a$
$(\mathbb{Z}_{12},+)$, $a=3$	$3+3=6$	9	0	$-3=9$
$(S_3,\circ)$, $a=f_5$	$f_5\circ f_5=f_6$	f_1	f_1	f_6

In an additive group the powers of a are its **multiples**, $a^n=na$, and $a^{-1}=-a$. "3^2" in $(\mathbb{Z}_{12},+)$ is 6, not 9.

[9] courses/math1061/cayley-tables.pdf
[10] courses/math1061/practice-problems.pdf

The power laws

For all $g \in G$ and all $i, j \in \mathbb{Z}$:

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

Why the first law holds. When i and j are both positive it is counting: i copies of g followed by j copies make $i + j$ copies. When the signs differ, the gs and g^{-1}s meet in the middle and cancel in pairs, $g * g^{-1} = e$, and what is left is the surplus. For example

$$g^3 * g^{-2} = g * g * \underbrace{g * g^{-1}}_{e} * g^{-1} = g * \underbrace{g * g^{-1}}_{e} = g = g^{3+(-2)}.$$

A zero power is e and changes nothing, matching $i + 0 = i$.

Why the second. i copies of g followed by i copies of g^{-1} cancel completely, so $g^i * g^{-i} = g^0 = e$, and in the other order $g^{-i} * g^i = g^0 = e$. That makes g^{-i} the inverse of g^i. And $(g^{-1})^i$ is i copies of g^{-1}, which is g^{-i} by definition.

The laws say powers in a group behave like powers of a number. They are what the cyclic subgroup needs.

Worked: one negative power, three ways

$[3]^{-4}$ in $(\mathbb{Z}_7 - \{[0]\}, \cdot)$, where $[3]^4 = [81] = [4]$ (2026-10-06-elementary-properties-of-groups[11]):

- **Invert, then power.** $[3]^{-1} = [5]$, because $[3] \cdot [5] = [15] = [1]$. So $[3]^{-4} = [5]^4 = [25] \cdot [25] = [4] \cdot [4] = [2]$.
- **Power, then invert.** $[3]^{-4} = ([3]^4)^{-1} = [4]^{-1} = [2]$, because $[4] \cdot [2] = [8] = [1]$.
- **Go round the loop.** The powers of $[3]$ are $[3], [2], [6], [4], [5], [1]$, so $[3]^6 = [1]$. Then $[3]^{-4} = [3]^{-4} \cdot [3]^6 = [3]^2 = [9] = [2]$.

All three give $[2]$. The third uses the fact that the powers in a finite group come round in a loop, which is the next section.

[11] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

When the powers repeat

In a finite group, some positive power of a is e. The powers $a, a^2, a^3, ...$ cannot all be different, so $a^i = a^j$ for some $0 < i < j$. Combine both sides with a^{-i}: $e = a^{j-i}$, a positive power.

Let n be the smallest positive integer with $a^n = e$. Then:

- $a, a^2, \ldots, a^n$ **are all different.** If $a^i = a^j$ with $1 \leq i < j \leq n$, the same step gives $a^{j-i} = e$ with $0 < j - i < n$, smaller than n.
- **After a^n the list repeats.** $a^{n+1} = a^n * a = e * a = a$, then $a^{n+2} = a^2$, and so on.
- **The negative powers are already in the list.** $a^{n-1} * a = a^n = e$, so $a^{-1} = a^{n-1}$, and in general $a^{-i} = a^{n-i}$. Going backwards round the loop meets the same elements.

So in a finite group

$$\langle a \rangle = \{a, a^2, a^3, \ldots, a^n = e\},$$

with exactly n elements: **list the positive powers until e appears, and stop.** (n is often called the order of a.) In an infinite group the powers need not repeat, and then the negative powers really are new.

The cyclic subgroup generated by a

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.**

Why it is a subgroup. The power laws are exactly the three checks.

- **Closure.** $a^i * a^j = a^{i+j}$, and $i + j \in \mathbb{Z}$, so it is in $\langle a \rangle$.
- **Identity.** $e = a^0 \in \langle a \rangle$.
- **Inverses.** $(a^i)^{-1} = a^{-i} \in \langle a \rangle$.

It is the smallest subgroup containing a. Suppose S is any subgroup with $a \in S$. Closure puts $a^2, a^3, a^4, ...$ in S. The identity puts $a^0 = e$ in S. Inverses put a^{-1} in S, and then closure puts $a^{-2}, a^{-3}, ...$ in S. So $\langle a \rangle \subseteq S$. A subgroup cannot contain a without containing all of its powers.

Two rules that save work:

- $\langle e \rangle = \{e\}$**.** Every power of the identity is the identity.

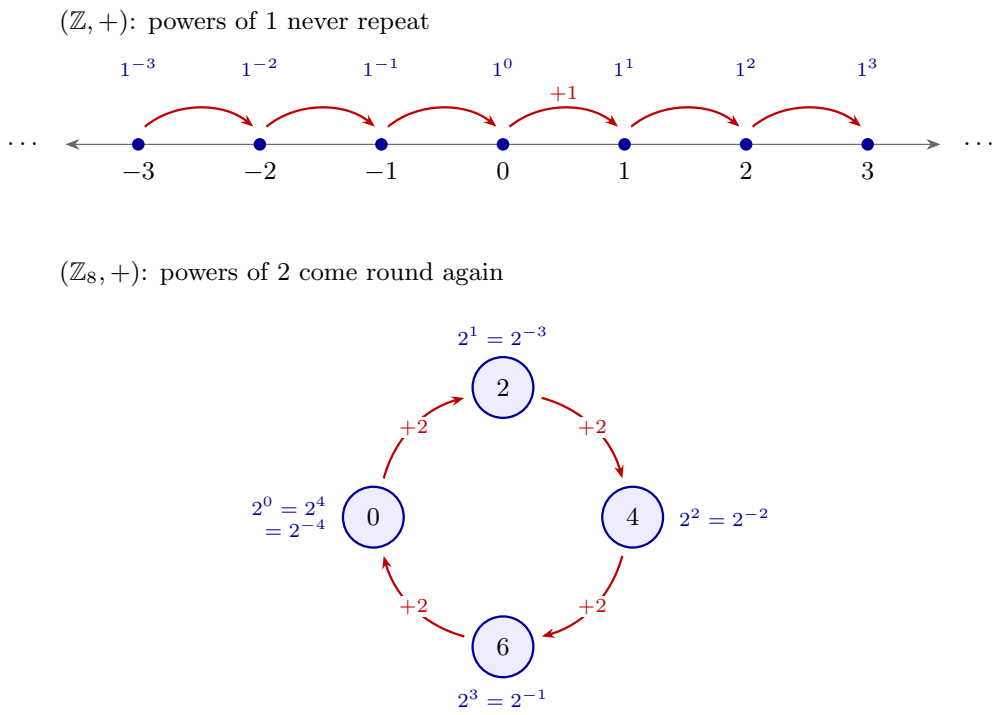


Figure 1: Powers of an element as steps, each step combining with the element once more; going left or backwards combines with its inverse. Top: in $(\mathbb{Z}, +)$ the powers of 1 run off in both directions and never repeat, so $\langle 1 \rangle$ needs the negative powers to reach $-1, -2, \ldots$. Bottom: in $(\mathbb{Z}_8, +)$ the powers of 2 come back to the identity at $2^4 = 0$, so the line closes into a loop of four. Every negative power lands on a positive one, such as $2^{-1} = 6 = 2^3$, and $\langle 2 \rangle = 2, 4, 6, 0$ is just the positive powers up to the identity.

- $\langle a \rangle = \langle a^{-1} \rangle$**.** The powers of a^{-1} are $(a^{-1})^i = a^{-i}$, and as i runs through all of $\mathbb{Z}$ so does $-i$. The same set, listed in the opposite order. In $(\mathbb{Z}_n, +)$ the inverse of a is $n - a$, so $\langle a \rangle = \langle n - a \rangle$.

To find $\langle a \rangle$ in a finite group, list $a, a^2, a^3, ...$, each one the previous one combined with a, until the identity appears (above).

Worked examples

$\langle 3 \rangle$ **in** $(\mathbb{Z}_{11} - \{[0]\}, \cdot)$**.** The powers are $3, 9, 27 = 5, 15 = 4, 12 = 1$, so $\langle 3 \rangle = \{1, 3, 4, 5, 9\}$, five of the ten elements. Worked and drawn in 2026-10-06-elementary-properties-of-groups[12].

All the cyclic subgroups of $(\mathbb{Z}_8, +)$ (2026-10-06-elementary-properties-of-groups[13]):

a	Powers of a until 0	$\langle a \rangle$	Size
0	0	$\{0\}$	1
1, 7	$1, 2, 3, 4, 5, 6, 7, 0$	$\mathbb{Z}_8$	8
3, 5	$3, 6, 1, 4, 7, 2, 5, 0$	$\mathbb{Z}_8$	8
2, 6	$2, 4, 6, 0$	$\{0, 2, 4, 6\}$	4
4	$4, 0$	$\{0, 4\}$	2

The rows pair each element with its inverse ($7 = -1$, $5 = -3$, $6 = -2$), which generates the same subgroup. Eight elements, four different cyclic subgroups, nested one inside the next: $\{0\} \subset \{0, 4\} \subset \{0, 2, 4, 6\} \subset \mathbb{Z}_8$.

All the cyclic subgroups of $(\mathbb{Z}_6, +)$**.** By the same method, $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$, $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$ and $\langle 3 \rangle = \{3, 0\}$. The subgroup $\langle 2 \rangle = \{0, 2, 4\}$ is the block in the table at 2026-10-06-elementary-properties-of-groups[14].

Cyclic groups

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

Such an a is a **generator** of G. A cyclic group is one in which **every element is a power of one element**.

- **To prove G is cyclic**, name a generator a and show every element of G is a power of it. In a finite group, list the powers of a until the identity appears and count: if there are $|G|$ different ones, $\langle a \rangle = G$.

[12] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[13] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[14] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

- **To prove G is not cyclic**, show that $\langle a \rangle \neq G$ for *every* $a \in G$. One element that fails to generate proves nothing.

Group	Cyclic?	Generators found	Where
$(\mathbb{Z}_{10}, +)$	yes	1	2026-10-06-elementary-properties-of-groups[15]
$(\mathbb{Z}_8, +)$	yes	$1, 3, 5, 7$	2026-10-06-elementary-properties-of-groups[16]
$(\mathbb{Z}_6, +)$	yes	$1, 5$	above
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	yes	$2, 3$	2026-10-06-elementary-properties-of-groups[17]
$(\mathbb{Z}_{11} - \{[0]\}, \cdot)$	yes	2, but not 3	practice-problems[18], Q4
$(\mathbb{Z}, +)$	yes	$1, -1$	2026-10-06-elementary-properties-of-groups[19]
$(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$	yes	$(1,1)$, $(1,2)$	below
$(\mathbb{Q}, +)$	**no**	none	below
$(S_3, \circ)$	**no**	none	symmetric-group[20]

$(\mathbb{Z}_n, +)$ **is always cyclic**, generated by 1: the powers of 1 are $1, 2, \ldots, n-1, n = 0$.

$(\mathbb{Z}, +)$ **needs the negative powers.** $\langle 1 \rangle = \{\ldots, 1^{-2}, 1^{-1}, 1^0, 1^1, 1^2, \ldots\} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}$. The positive powers alone give only $\mathbb{Z}^+$.

A cyclic group is abelian. Any two elements are powers a^i and a^j of the generator, and $a^i * a^j = a^{i+j} = a^{j+i} = a^j * a^i$. So a non-abelian group, such as S_3, cannot be cyclic.

Worked: $(\mathbb{Q}, +)$ is not cyclic

In $(\mathbb{Q}, +)$ the powers of a are its integer multiples, $\langle a \rangle = \{na : n \in \mathbb{Z}\}$. Take any $a \in \mathbb{Q}$.

- If $a = 0$, then $\langle a \rangle = \{0\} \neq \mathbb{Q}$.

[15] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[16] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[17] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[18] courses/math1061/practice-problems.pdf
[19] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[20] courses/math1061/symmetric-group.pdf

- If $a = \frac{p}{q} \neq 0$, with $p, q \in \mathbb{Z}$ and $q \neq 0$, then $\frac{p}{2q} \in \mathbb{Q}$. If it were in $\langle a \rangle$, then $\frac{p}{2q} = n \cdot \frac{p}{q}$ for some $n \in \mathbb{Z}$, and dividing by $\frac{p}{q} \neq 0$ gives $n = \frac{1}{2}$, which is not an integer. So $\frac{p}{2q} \notin \left\langle \frac{p}{q} \right\rangle$.

No a generates $\mathbb{Q}$, so $(\mathbb{Q}, +)$ is not cyclic. The same argument works for $(\mathbb{R}, +)$.

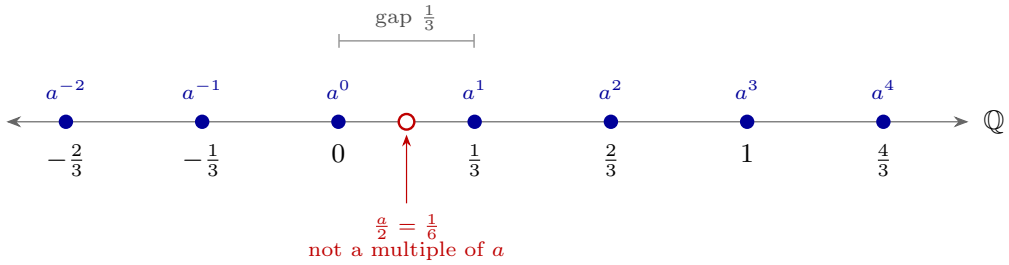


Figure 2: Why no rational number generates $(\mathbb{Q}, +)$, drawn for $a = \frac{1}{3}$. The powers of a under addition are its integer multiples, evenly spaced points a distance $\frac{1}{3}$ apart running off in both directions. Half of a, here $\frac{1}{6}$, is a rational number that falls in the gap between $a^0 = 0$ and $a^1 = \frac{1}{3}$, so it is not a power of a. Any other non-zero a has gaps of the same kind, and $a = 0$ generates only 0.

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

In $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$, with $(a, b) + (c, d) = ((a + c) \bmod 2,\ (b + d) \bmod 3)$, the powers of $(1, 1)$ are

$$(1, 1),\ (0, 2),\ (1, 0),\ (0, 1),\ (1, 2),\ (0, 0),$$

six different elements, so $\langle (1, 1) \rangle$ is the whole group and it is cyclic (2026-10-06-elementary-properties-of-groups[21]). Each step adds 1 to both coordinates. The first coordinate is back at 0 after every 2 steps, the second after every 3, and both are back together for the first time after 6, so the powers visit all six pairs before returning to $(0, 0)$. Elements that move only one coordinate generate smaller subgroups:

$(1, 2)$ is a second generator, since it is the inverse of $(1, 1)$: $(1, 1) + (1, 2) = (2 \bmod 2,\ 3 \bmod 3) = (0, 0)$. Of the other non-identity elements, $(0, 1)$ and its inverse $(0, 2)$ both generate $\langle (0, 1) \rangle$, and $(1, 0)$, which is its own inverse, generates $\langle (1, 0) \rangle$.

[21] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

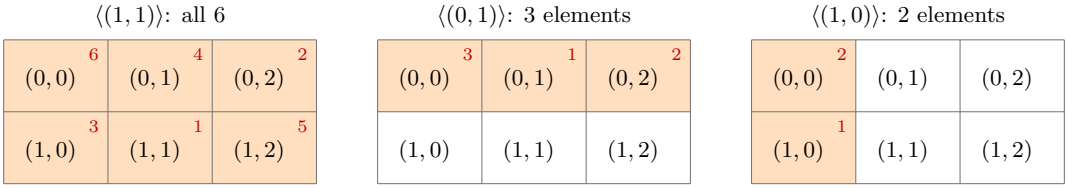


Figure 3: Three cyclic subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_3$, each shaded inside the six-element group. A shaded cell is a power of the generator, and the small number in its corner is the k at which the generator's kth power first lands there. Left: $(1,1)$ changes both coordinates at every step and reaches all six pairs before $(1,1)^6 = (0,0)$, so it generates the whole group and the group is cyclic. Middle: $(0,1)$ never changes the first coordinate, so its powers stay in the top row and $\langle(0,1)\rangle$ has three elements. Right: $(1,0)$ never changes the second coordinate, so $\langle(1,0)\rangle = (0,0), (1,0)$.

Common mistakes

- **Checking associativity for a subgroup.** It is inherited from G and never fails. The three that need checking are closure, identity and inverses.
- **Forgetting that e must be in H.** $\mathbb{R} - \{0\}$ fails as a subgroup of $(\mathbb{R}, +)$ because the identity was removed.
- **Changing the operation.** A subgroup of $(G, *)$ uses $*$. $(\mathbb{R} - \{0\}, \cdot)$ is a group, but not a subgroup of $(\mathbb{R}, +)$.
- **Reading a^2 as $a \cdot a$ in an additive group.** In $(\mathbb{Z}_{12}, +)$, $3^2 = 3 + 3 = 6$.
- **Reading a^{-1} as $\frac{1}{a}$.** It is the inverse under the group's operation: $-a$ in an additive group.
- **Leaving out the negative powers in an infinite group.** The positive powers of 1 in $(\mathbb{Z}, +)$ are only $1, 2, 3, \ldots$.
- **Confusing $\langle a \rangle$ with $\{a\}$.** $\langle a \rangle$ contains every power of a, including e.
- **"3 does not generate it, so it is not cyclic."** One generator is enough to be cyclic. $\mathbb{Z}_{11} - \{[0]\}$ is $\langle 2 \rangle$ though not $\langle 3 \rangle$. To show a group is not cyclic, every element must fail.
- **Expecting the identity to generate.** $\langle e \rangle = \{e\}$, in every group.

See also

- groups[22] — the four properties, and the elementary properties such as the unique identity and $(g * h)^{-1} = h^{-1} * g^{-1}$
- cayley-tables[23] — a subgroup as a block of the table, when its elements are listed first
- integers-modulo-n[24] — $\mathbb{Z}_n$ and $\mathbb{Z}_n - \{[0]\}$, where most of the cyclic examples live

[22] courses/math1061/groups.pdf
[23] courses/math1061/cayley-tables.pdf
[24] courses/math1061/integers-modulo-n.pdf

- symmetric-group[25] — the cyclic subgroups of S_3, a group that is not cyclic
- 2026-10-06-elementary-properties-of-groups[26] — Lecture 27 · 2026-10-08-definitions-and-examples-of-fields[27] — Lecture 28
- practice-problems[28] — §34, with full worked solutions

[25] courses/math1061/symmetric-group.pdf
[26] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[27] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[28] courses/math1061/practice-problems.pdf