Lecture 26 — Definitions and Examples of Groups

Table of contents

Goals . . . 1
Modular arithmetic and the group $\mathbb{Z}_n$ . . . 2
The definition of a group . . . 3
Worked: which of these are groups? . . . 3
Worked: a multiplication table mod 7 . . . 4
The symmetric group S_n . . . 5
Worked: the Cayley table of S_3 . . . 7
S_3 is a non-abelian group . . . 9
Worked: no repeats in a row . . . 12
See also . . . 12

What a group is, how to check the four properties, and three families of examples: number systems, the integers modulo n, and the symmetric group. Pre-work: Video 033 (Definitions and Examples of Groups). The definition and the examples are collected in groups[1], $\mathbb{Z}_n$ and arithmetic with equivalence classes in integers-modulo-n[2], reading a group off its table in cayley-tables[3], and S_n and S_3 in symmetric-group[4].

Goals

1. Gain familiarity with **groups**.
2. Learn how to prove group properties.
3. Investigate some examples of groups.

Three questions to keep in mind:

[1] courses/math1061/groups.pdf
[2] courses/math1061/integers-modulo-n.pdf
[3] courses/math1061/cayley-tables.pdf
[4] courses/math1061/symmetric-group.pdf

- **How do addition and multiplication of equivalence classes work in $\mathbb{Z}_n$?** The next section.
- **What exactly is the symmetric group?** Below.
- **What group operations are there besides addition and multiplication?** Composition of functions is one, in the symmetric group. Subtraction is one that fails, in the list of candidates.

Modular arithmetic and the group $\mathbb{Z}_n$

For any $n \in \mathbb{Z}^+$, $(\mathbb{Z}_n, +)$ is a group. Its elements are equivalence classes.

Fix $d \in \mathbb{Z}^+$ and take the equivalence relation R on $\mathbb{Z}$ defined by: for all $m, n \in \mathbb{Z}$,

$$m \, R \, n \iff m \equiv n \pmod{d} \iff d \mid (m-n).$$

Then $\{[0], [1], [2], \dots, [d-1]\}$ is a partition of $\mathbb{Z}$ (equivalence-classes-and-partitions[5]). $\mathbb{Z}_n$ is this set of classes for congruence mod n.

For $n = 10$:

$$\mathbb{Z}_{10} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9]\}$$

$$[0] = \{x \in \mathbb{Z} : x \equiv 0 \pmod{10}\} = \{\dots, -30, -20, -10, 0, 10, 20, 30, \dots\}$$

$$[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod{10}\} = \{\dots, -29, -19, -9, 1, 11, 21, 31, \dots\}$$

Any element of a class can be used to name it, so $[0] = [10] = [30]$ and $[1] = [21]$. The usual names are $[0], [1], \dots, [n-1]$.

The operations. Define $+$ and $\cdot$ on $\mathbb{Z}_n$ by: for all $[a], [b] \in \mathbb{Z}_n$,

$$[a] + [b] = [a + b] \qquad \text{and} \qquad [a] \cdot [b] = [ab].$$

When doing arithmetic in $\mathbb{Z}_n$, any representative of an equivalence class can be used.

[5] courses/math1061/equivalence-classes-and-partitions.pdf

Example. In $\mathbb{Z}_{10}$:

$$\begin{aligned}([8]+[9])\cdot([6]+[7]) &= ([8]+[-1])\cdot([6]+[-3]) \\ &= [7]\cdot[3] \\ &= [7\cdot 3] \\ &= [21] \\ &= [1]\end{aligned}$$

The first line swaps [9] for [−1] and [7] for [−3]. They are the same classes, because $9 \equiv -1$ and $7 \equiv -3 \pmod{10}$, and the smaller numbers are easier to work with. Keeping the original representatives gives $[17]\cdot[13] = [221] = [1]$, the same class. Why the answer never depends on the representative is in integers-modulo-n[6].

The definition of a group

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

Worked: which of these are groups?

	Group?	Why
$(\mathbb{Z}, +)$	**Yes**	
$(\mathbb{Z} - \{0\}, \cdot)$	**No**	2 has no inverse. The identity would have to be 1, and $2 \cdot y = 1$ needs $y = \frac{1}{2} \notin \mathbb{Z}$
$(\mathbb{Z}, -)$	**No**	not associative: $(3-2)-1 = 0$ but $3-(2-1) = 2$
$(\mathbb{Z}_3, +)$	**Yes**	
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	**Yes**	
$(\mathbb{R}, +)$	**Yes**	closed, associative, identity 0, $x^{-1} = -x$

[6] courses/math1061/integers-modulo-n.pdf

	Group?	Why
$(\mathbb{R}, \cdot)$	**No**	0 has no inverse. The identity would have to be 1, and $0 \cdot y = 1$ has no solution
$(\mathbb{R} - \{0\}, \cdot)$	**Yes**	closed, associative, identity 1, $x^{-1} = \frac{1}{x}$ (and $x \neq 0$)

Three things to notice:

- **One failed property is enough for a *No*,** and it is shown with specific elements: the element 2 for inverses, the numbers 3, 2, 1 for associativity.
- **The inverse depends on the operation.** In $(\mathbb{R}, +)$ the inverse of x is $-x$, written $x^{-1} = -x$. The superscript -1 is the notation for "the inverse in this group". It is not a reciprocal unless the operation is multiplication.
- **Removing one element can repair a set.** $(\mathbb{R}, \cdot)$ fails only because of 0. Taking 0 out gives $(\mathbb{R} - \{0\}, \cdot)$, which is a group.

Each line is checked against all four properties in groups[7].

Why inverses matter. Solving $2x = 4$ is done by applying an inverse to both sides:

$$2x = 4 \quad \Longrightarrow \quad 2^{-1} \cdot 2x = 2^{-1} \cdot 4 \quad \Longrightarrow \quad x = 2.$$

In a group that can always be done (groups[8]).

Worked: a multiplication table mod 7

(a) Write out the Cayley table for $\mathbb{Z}_7 - \{[0]\}$ with operation multiplication modulo 7.

(b) Verify the four group properties to show that $(\mathbb{Z}_7 - \{[0]\}, \cdot)$ is a group. You may assume associativity.

The set is $\mathbb{Z}_7 - \{[0]\} = \{[1], [2], [3], [4], [5], [6]\}$.

(a) Each entry is a product reduced mod 7. For example $[2] \cdot [5] = [10] = [3]$ and $[2] \cdot [6] = [12] = [5]$.

[7] courses/math1061/groups.pdf
[8] courses/math1061/groups.pdf

$\cdot$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

(b)

- **Closure.** The body of the table uses only $[1], [2], [3], [4], [5], [6]$. ✓
- **Associativity.** Given.
- **Identity.** $[1]$, since $[1] \cdot g = g \cdot [1] = g$ for all $g \in \mathbb{Z}_7 - \{[0]\}$.
- **Inverses.** $[1]^{-1} = [1]$, $[2]^{-1} = [4]$, $[3]^{-1} = [5]$, $[4]^{-1} = [2]$, $[5]^{-1} = [3]$, $[6]^{-1} = [6]$.

So $(\mathbb{Z}_7 - \{[0]\}, \cdot)$ is a group.

> 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.

Here $[a][b] = [b][a]$, so this group is abelian.

Each property can be read straight off the table:

- **Identity.** The row and the column of $[1]$ repeat the headings.
- **Inverses.** Find the $[1]$ in a row. In the row of $[3]$ it is in the column of $[5]$, so $[3] \cdot [5] = [1]$ and $[3]^{-1} = [5]$.
- **Abelian.** The table is the same on both sides of the main diagonal.

The symmetric group S_n

> S_n is the group consisting of the set of all bijections from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$, together with the binary operation $\circ$, composition of functions.

The elements of this group are functions, and the operation is "do one, then the other". Bijections are the functions of one-to-one-and-onto-functions[9], and composition is composition-of-functions[10].

How many elements? A bijection can send 1 to any of 3 places. That leaves 2 places for 2 and 1 for 3, so S_3 has $3 \cdot 2 \cdot 1 = 6$ elements.

[9] courses/math1061/one-to-one-and-onto-functions.pdf
[10] courses/math1061/composition-of-functions.pdf

$\cdot$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

Figure 1: The Cayley table of $\mathbb{Z}_7 - [0]$ under multiplication mod 7, with three things marked. Yellow: the row and the column of [1] repeat the headings, so [1] is the identity. Red rings: every row and every column contains [1] exactly once, and its position gives an inverse. The ring in row [2] is in column [4], so $[2]^{-1} = [4]$. Grey: the main diagonal. The table is its own mirror image in it, so $[a][b] = [b][a]$ and the group is abelian.

Three elements of S_3:

	As a set of pairs	Values
f_1	$\{(1,1),(2,2),(3,3)\}$	$f_1(1)=1,\ f_1(2)=2,$ $f_1(3)=3$
f_2	$\{(1,2),(2,1),(3,3)\}$	$f_2(1)=2,\ f_2(2)=1,$ $f_2(3)=3$
f_3	$\{(1,3),(2,2),(3,1)\}$	$f_3(1)=3,\ f_3(2)=2,$ $f_3(3)=1$

Composing two of them. $(f_1 \circ f_2)(x) = f_1(f_2(x))$, so

$$(f_1 \circ f_2)(1) = f_1(f_2(1)) = f_1(2) = 2$$
$$(f_1 \circ f_2)(2) = f_1(f_2(2)) = f_1(1) = 1$$
$$(f_1 \circ f_2)(3) = f_1(f_2(3)) = f_1(3) = 3$$

and so $f_1 \circ f_2 = f_2$.

In $f_1 \circ f_2$ the function on the right, f_2, acts first. A picture of the composition reads left to right in the order things happen, f_2 and then f_1, while the formula reads right to left. f_1 sends everything to itself, so composing with it changes nothing, and $f_1 \circ f_2 = f_2$.

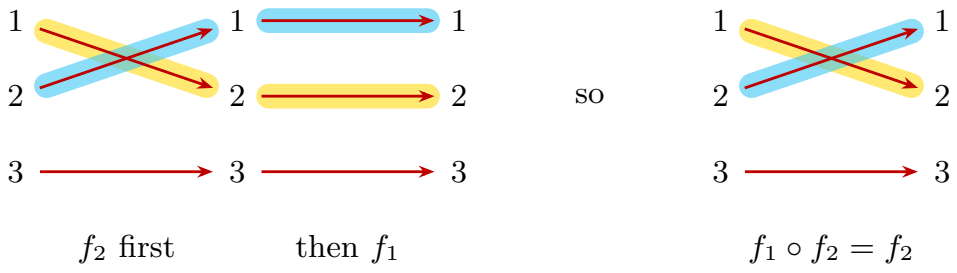


Figure 2: $f_1 \circ f_2$ in two steps. Follow each number through f_2 first and then through f_1. The yellow route takes 1 to 2 and then leaves it at 2, so $(f_1 \circ f_2)(1) = 2$. The cyan route takes 2 to 1 and leaves it there, so $(f_1 \circ f_2)(2) = 1$. Joining the start of each route directly to its end gives the single diagram on the right, which is f_2.

Worked: the Cayley table of S_3

Complete the Cayley table for S_3.

The six elements of S_3:

	$1 \mapsto$	$2 \mapsto$	$3 \mapsto$
f_1	1	2	3
f_2	2	1	3
f_3	3	2	1
f_4	1	3	2
f_5	2	3	1
f_6	3	1	2

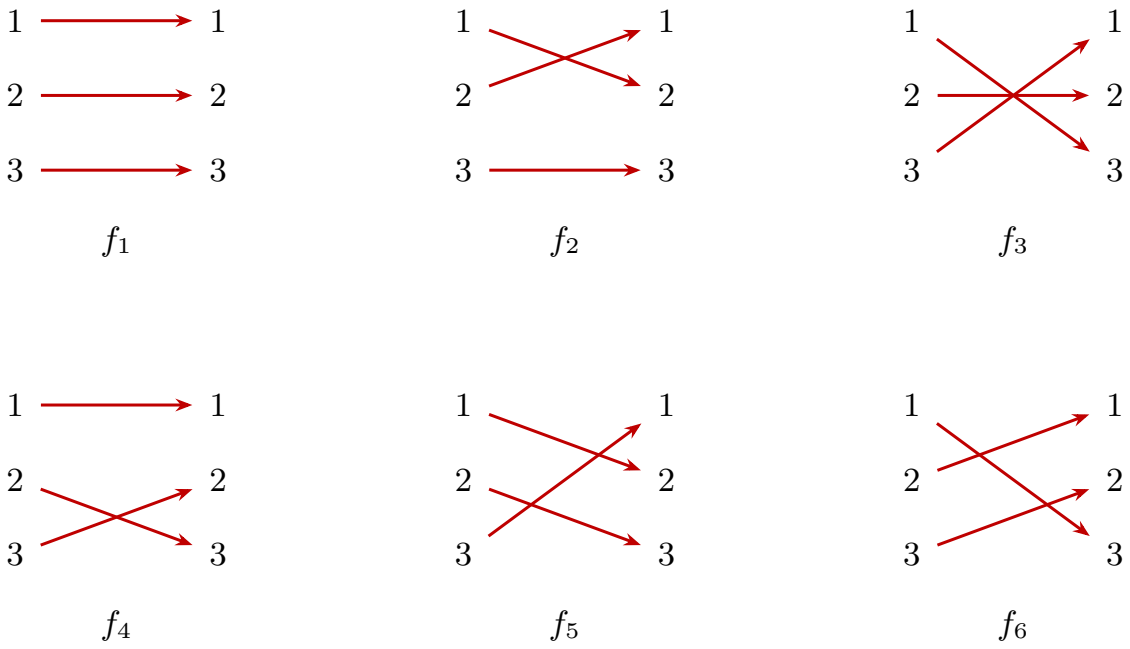


Figure 3: The six elements of S_3, every bijection from $1, 2, 3$ to itself. f_1 moves nothing. f_2, f_3 and f_4 each swap two numbers and leave the third alone: f_2 swaps 1 and 2, f_3 swaps 1 and 3, f_4 swaps 2 and 3. f_5 and f_6 move all three numbers round, in opposite directions.

The table. The ten entries to be found are in bold. The rest are given.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	$\mathbf{f}_4$	f_6	f_5	f_1	f_3	f_2
f_5	$\mathbf{f}_5$	$\mathbf{f}_3$	$\mathbf{f}_4$	$\mathbf{f}_2$	f_6	f_1
f_6	$\mathbf{f}_6$	$\mathbf{f}_4$	$\mathbf{f}_2$	$\mathbf{f}_3$	$\mathbf{f}_1$	f_5

The entry in the row of f and the column of g is $f \circ g$. The row comes first as written, and the column's function is the one that acts first.

Two entries worked in full:

- $f_2 \circ f_3 = f_6$**.** Do f_3 first and then f_2. The entry is in the row of f_2 and the column of f_3.
- $f_5 \circ f_3 = f_4$**.** Do f_3 first and then f_5. The entry is in the row of f_5 and the column of f_3.

The order matters. The entry in the row of f_3 and the column of f_2 is $f_3 \circ f_2 = f_5$. It is the mirror image of $f_2 \circ f_3 = f_6$ in the table, and it is a different element.

S_3 is a non-abelian group

Checking the properties one at a time, with $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.

Closure. For all $f, g \in G$, $f \circ g \in G$. ✓ Every entry of the table is one of the six.

Associativity. For all $f, g, h \in G$, $f \circ (g \circ h) = (f \circ g) \circ h$. ✓ For any x,

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x).$$

Both bracketings send x to $f(g(h(x)))$. This works for any three functions, so composition of functions is always associative and nothing about S_3 in particular has to be checked.

Identity. There is an $f \in G$ with $f \circ g = g \circ f = g$ for all $g \in G$: f_1 **is the identity.**

Inverses. For every $f \in G$ there is an $f^{-1} \in G$ with $f \circ f^{-1} = f^{-1} \circ f = f_1$:

$$f_1^{-1} = f_1, \quad f_2^{-1} = f_2, \quad f_3^{-1} = f_3, \quad f_4^{-1} = f_4, \quad f_5^{-1} = f_6, \quad f_6^{-1} = f_5.$$

So S_3 is a group.

Abelian? That would need $f \circ g = g \circ f$ for all $f, g \in G$. But $f_2 \circ f_3 = f_6$ and $f_3 \circ f_2 = f_5$, so this group is **not abelian**. Being abelian is a "for all", so one pair that fails settles it.

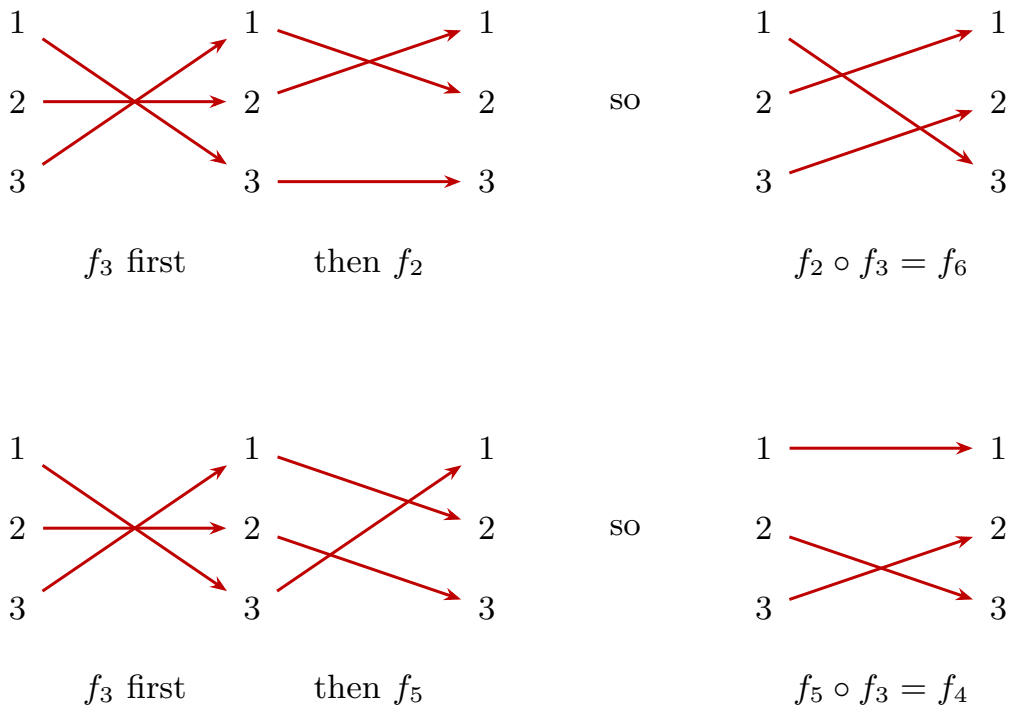


Figure 4: Two entries of the table, worked out. Top: $f_2 \circ f_3$. Do f_3 first, then f_2: 1 goes to 3 and stays, 2 stays and then goes to 1, 3 goes to 1 and then to 2. Overall $1 \to 3$, $2 \to 1$, $3 \to 2$, which is f_6. Bottom: $f_5 \circ f_3$. Do f_3 first, then f_5: 1 goes to 3 and then back to 1, 2 stays and then goes to 3, 3 goes to 1 and then to 2. Overall $1 \to 1$, $2 \to 3$, $3 \to 2$, which is f_4.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

$f_2 \circ f_3 = f_6$

$f_3 \circ f_2 = f_5$

Figure 5: The Cayley table of S_3, the entry in the row of f and the column of g being $f \circ g$. Yellow: the row and column of f_1 repeat the headings, so f_1 is the identity. Red rings: f_1 appears once in every row and column. Four of the rings are on the diagonal, so f_1, f_2, f_3 and f_4 are their own inverses, and the other two show that f_5 and f_6 are inverses of each other. The two boxed entries are mirror images in the main diagonal, shaded grey, and they differ: $f_2 \circ f_3 = f_6$ but $f_3 \circ f_2 = f_5$. The table is not symmetric, so the group is not abelian.

Worked: no repeats in a row

> Use the group properties to prove that in a Cayley table for a group, the elements in each row are distinct.

A repeat in a row would be the same element x in two different columns b and c of the row of a. So suppose that, and get a contradiction.

Proof (by contradiction). Suppose $(G, *)$ is a group with identity e. Let $a, b, c, x \in G$ and suppose $a * b = a * c = x$ with $b \neq c$. We have

$$\begin{aligned} a * b &= a * c && \\ a^{-1} * (a * b) &= a^{-1} * (a * c) && \text{since } a^{-1} \text{ exists in } G \\ (a^{-1} * a) * b &= (a^{-1} * a) * c && \text{associativity} \\ e * b &= e * c && \text{inverses} \\ b &= c && \text{identity} \end{aligned}$$

This contradicts $b \neq c$. So the elements in each row are distinct. ■

A similar argument shows that the elements in each column are distinct.

Every step is licensed by one of the group properties, named at the right, and the proof uses three of the four: inverses, associativity and identity. It is the working of $2x = 4$, so $x = 2$, carried out in any group: **apply a^{-1} on the left of both sides and a cancels**. The column version and what the result means for a table are in cayley-tables[11].

See also

- groups[12] — the four properties, abelian groups, and the eight candidates checked one by one
- integers-modulo-n[13] — $\mathbb{Z}_n$ as a set of equivalence classes, and why any representative can be used
- cayley-tables[14] — reading identity, inverses and commutativity off a table, and why rows and columns have no repeats
- symmetric-group[15] — S_n, the six elements of S_3, and composing them

[11] courses/math1061/cayley-tables.pdf
[12] courses/math1061/groups.pdf
[13] courses/math1061/integers-modulo-n.pdf
[14] courses/math1061/cayley-tables.pdf
[15] courses/math1061/symmetric-group.pdf

- composition-of-functions[16] · one-to-one-and-onto-functions[17] — the operation and the elements of S_n
- 2026-09-22-partial-order-relations[18] — Lecture 25 · 2026-10-06-elementary-properties-of-groups[19] — Lecture 27
- practice-problems[20] — §33, with full worked solutions

[16] courses/math1061/composition-of-functions.pdf
[17] courses/math1061/one-to-one-and-onto-functions.pdf
[18] courses/math1061/2026-09-22-partial-order-relations.pdf
[19] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[20] courses/math1061/practice-problems.pdf