Cayley Tables

Table of contents

What a Cayley table is 1
Reading the properties off a table 2
Rows and columns have no repeats 2
Subgroups in a table 5
The tables in the course so far 5
Common mistakes 6
See also 6

A Cayley table writes out every product in a finite set with an operation. For a group, most of the definition can be read straight off it. The definition is in groups[1]. The tables for $\mathbb{Z}_7 - \{[0]\}$ and for S_3 are built in 2026-09-24-definitions-and-examples-of-groups[2]. With the right ordering of the headings, a subgroup shows up as a block of the table (below, and subgroups-and-cyclic-groups[3]).

What a Cayley table is

One row and one column for each element, in the same order, with the operation's symbol in the corner. **The entry in the row of g and the column of h is $g * h$**: row first, then column.

The order matters whenever the operation is not commutative. In the table of S_3 the entry in row f_2, column f_3 is f_6, so $f_2 \circ f_3 = f_6$ (2026-09-24-definitions-and-examples-of-groups[4]). The entry in row f_3, column f_2 is a different element, f_5.

[1] courses/math1061/groups.pdf
[2] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[3] courses/math1061/subgroups-and-cyclic-groups.pdf
[4] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

Reading the properties off a table

Property	What to look for in the table
closure	The body uses only the elements in the headings.
associativity	Cannot be seen. It has to be argued separately, or be given.
identity	A row that repeats the column headings **and** a column that repeats the row headings, belonging to the same element.
inverses	The identity e appears in every row. If e is in row g and column h, then $g * h = e$.
abelian	The table is its own mirror image in the main diagonal (top left to bottom right).

For $\mathbb{Z}_7 - \{[0]\}$ the checks read: closure, because the body of the table uses only $[1], \ldots, [6]$; associativity, given; identity [1], since $[1] \cdot g = g \cdot [1] = g$; and six inverses, one from each [1] in the body (2026-09-24-definitions-and-examples-of-groups[5]).

Three details:

- **Identity needs the row and the column.** The row of e shows $e * g = g$, and the column shows $g * e = g$. The definition asks for both.
- **Inverses need both orders too.** $g * h = e$ and $h * g = e$ are two different cells, mirror images of each other. So the es in a group's table are placed symmetrically about the diagonal, even when the table as a whole is not symmetric. In S_3, $f_5 \circ f_6 = f_1$ and $f_6 \circ f_5 = f_1$.
- **An e on the diagonal** means an element is its own inverse. In $\mathbb{Z}_7 - \{[0]\}$ those are [1] and [6].

The figure below marks the same three things on a second table, the one for $\mathbb{Z}_5 - \{[0]\}$ from practice-problems[6], Q4.

Rows and columns have no repeats

> In a Cayley table for a group, the elements in each row are distinct.
> A similar argument shows that the elements in each column are distinct.

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

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

identity: 1

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

inverses: $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

abelian: symmetric in the diagonal

Figure 1: Three readings of one table, $\mathbb{Z}_5 - [0]$ under multiplication, written without brackets. Left: the row and the column of 1, in yellow, repeat the headings, so 1 is the identity. Middle: the identity appears once in every row. The ring in row 2 is in column 3, so $2^{-1} = 3$; the rings on the diagonal show that 1 and 4 are their own inverses. Right: each entry equals its mirror image in the shaded diagonal, such as the two boxed 3s and the two boxed 2s, so the operation is commutative and the group is abelian.

Rows. By contradiction (2026-09-24-definitions-and-examples-of-groups[7]). Suppose row a has the same entry x in two different columns $b \neq c$, so $a * b = a * c$. Apply a^{-1} on the **left** of both sides:

$$a^{-1} * (a * b) = a^{-1} * (a * c) \implies (a^{-1} * a) * b = (a^{-1} * a) * c \implies e * b = e * c \implies b = c,$$

using inverses, associativity, inverses and identity in turn. That contradicts $b \neq c$. ($\Rightarrow\Leftarrow$)

Columns. The "similar argument", written out. Suppose column a has the same entry in two different rows $b \neq c$, so $b * a = c * a$. Now a is on the right, so apply a^{-1} on the **right**:

$$(b * a) * a^{-1} = (c * a) * a^{-1} \implies b * (a * a^{-1}) = c * (a * a^{-1}) \implies b * e = c * e \implies b = c,$$

a contradiction again. The figure below shows both cases.

The two results are **cancellation**: from $a * b = a * c$ conclude $b = c$, and from $b * a = c * a$ conclude $b = c$. The a being cancelled must be on the same side in both products. $a * b = c * a$ does not give $b = c$ unless the group is abelian.

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

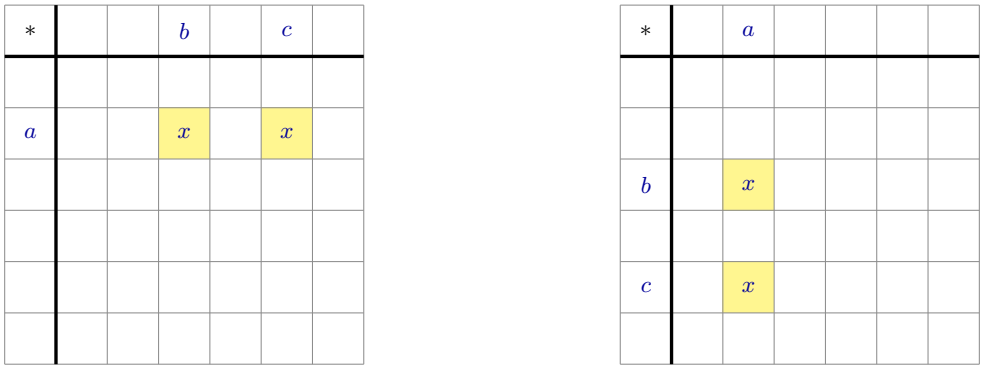


Figure 2: What the two results forbid. Left: the same element x twice in the row of a, in the columns of two different elements b and c. That would mean $a * b = a * c$, and applying a^{-1} on the left gives $b = c$. Right, the column version: the same x twice in the column of a, which would mean $b * a = c * a$, and applying a^{-1} on the right gives $b = c$. Neither picture can occur in the table of a group.

What it gives for a finite table

In a group with n elements, a row has n entries, all different, all taken from the n elements. So **every element appears exactly once in every row**, and likewise in every column. Check it against the tables for $\mathbb{Z}_7 - \{[0]\}$ and S_3. Three uses:

- **Finishing a table.** A row with one empty cell must be completed by the one element not yet in it. Suppose the last row of the S_3 table has only f_5 filled in, in its last cell, and the other five cells empty. Once four of them are worked out, f_6, f_4, f_2, f_3, the remaining one must be f_1.
- **Spotting a non-group.** A repeat in a row or a column means the table is not a group's. Multiplication mod 9 on $\{1, \ldots, 8\}$ has $3 \cdot 1 = 3$ and $3 \cdot 4 = 12 \equiv 3$ in the row of 3. That set is also not closed, since $3 \cdot 3 \equiv 0$ (practice-problems[8], Q1).
- **Finding inverses.** e appears exactly once in each row, so each element has exactly one inverse to read off.

No repeats does **not** show that a table is a group's. Associativity still cannot be seen in a table.

[8] courses/math1061/practice-problems.pdf

Subgroups in a table

A subgroup is a subset that is a group under the same operation (subgroups-and-cyclic-groups[9]). To see one in a table, **list its elements first**, in the same order along the top and down the side. Then the top-left block of the table holds every product of two of its elements: it is the subgroup's own table, and the checks are read off the block.

Check	What to look for in the block
closure	The body of the block uses only the block's own headings.
identity	The identity of the group is among the block's headings.
inverses	The identity appears in every row of the block.
associativity	Nothing to check: it is inherited from the whole group.

$(\mathbb{Z}_6, +)$ with $[0], [2], [4]$ listed first is drawn in 2026-10-06-elementary-properties-of-groups[10]. The same works in a non-abelian group. In S_3, list f_1, f_5, f_6 first:

$\{f_1, f_5, f_6\}$ is every power of f_5, since $f_5^2 = f_6$ and $f_5^3 = f_1$, so it is the cyclic subgroup $\langle f_5 \rangle$ (symmetric-group[11]).

A subset that is not a subgroup leaks. List f_1, f_2, f_3 first instead. The block then contains $f_2 \circ f_3 = f_6$, which is not one of its headings, so $\{f_1, f_2, f_3\}$ is not closed and is not a subgroup. In $\mathbb{Z}_6$, the block for $\{[0], [1]\}$ contains $[1] + [1] = [2]$, and fails the same way.

The tables in the course so far

Group	Elements	Abelian?	Where
$(\mathbb{Z}_7 - \{[0]\}, \cdot)$	6	yes	2026-09-24-definitions-and-examples-of-groups[12]
$(S_3, \circ)$	6	**no**	2026-09-24-definitions-and-examples-of-groups[13]

[9] courses/math1061/subgroups-and-cyclic-groups.pdf
[10] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[11] courses/math1061/symmetric-group.pdf
[12] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[13] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

Group	Elements	Abelian?	Where
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	4	yes	practice-problems[14], Q4; above
$(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$	4	yes	the same practice set, Q5
$(\mathbb{Z}_3, +)$	3	yes	integers-modulo-n[15]
$(\mathbb{Z}_6, +)$, even classes first	6	yes	2026-10-06-elementary-properties-of-groups[16]
$(S_3, \circ)$, f_1, f_5, f_6 first	6	**no**	above

The first two have the same number of elements and are different kinds of group: one is abelian and the other is not. The size of a group does not determine it.

Common mistakes

- **Reading the entry as column $*$ row.** It is row $*$ column. For an abelian group the mistake is invisible. For S_3 it gives wrong answers.
- **Listing the rows and columns in different orders.** The diagonal symmetry test needs the same order on both.
- **Claiming the identity from its row alone.**
- **"The table has no repeats, so it is a group."** Closure, identity and inverses can be read off. Associativity cannot.
- **Forgetting closure.** An entry in the body that is not one of the headings ends the matter at once.

See also

- groups[17] — the four properties the table is checked against, and cancellation as solving $a * x = b$
- integers-modulo-n[18] — the groups $\mathbb{Z}_n$ and $\mathbb{Z}_n - \{[0]\}$ behind the first tables
- symmetric-group[19] — S_3, whose table is not symmetric
- subgroups-and-cyclic-groups[20] — subgroups and cyclic subgroups, the blocks found above

[14] courses/math1061/practice-problems.pdf
[15] courses/math1061/integers-modulo-n.pdf
[16] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[17] courses/math1061/groups.pdf
[18] courses/math1061/integers-modulo-n.pdf
[19] courses/math1061/symmetric-group.pdf
[20] courses/math1061/subgroups-and-cyclic-groups.pdf

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

Figure 3: The Cayley table of S_3 with f_1, f_5, f_6 listed first; the entry in the row of f and the column of g is $f \circ g$. The outlined top-left block uses only f_1, f_5, f_6, so that set is closed under composition. It contains the identity f_1, and the rings show f_1 in every row of the block, so each of the three has its inverse among them: $f_5 \circ f_6 = f_6 \circ f_5 = f_1$. So f_1, f_5, f_6 is a subgroup of S_3. Shaded cells hold f_1, f_5 or f_6. As with the even classes of $\mathbb{Z}_6$, the table falls into four blocks, each using only the subgroup's elements or only the other three.

- proof-techniques[21] — proof by contradiction, the method of the rows result
- 2026-09-24-definitions-and-examples-of-groups[22] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[23] — Lecture 27 · 2026-10-08-definitions-and-examples-of-fields[24] — Lecture 28, where the table of $\mathbb{Z}_4 - \{[0]\}$ fails closure
- practice-problems[25] — §33, with full worked solutions

[21] courses/math1061/proof-techniques.pdf
[22] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[23] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[24] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[25] courses/math1061/practice-problems.pdf