MATH1061 — Week 9 Notes

Table of contents

Lecture 24 — Equivalence Relations **1**
- Goals . . . 1
- Three questions to start with . . . 3
- The definition . . . 3
- Worked: the sum is rational . . . 3
- Worked: the difference is rational . . . 4
- Partitions . . . 5
- Equivalence classes . . . 6
- Worked: the classes of τ . . . 7
- Two classes are equal or disjoint . . . 9
- Worked: a relation defined with "or" . . . 10
- From a partition to an equivalence relation . . . 11
- See also . . . 12

Lecture 25 — Partial Order Relations **13**
- Goals . . . 13
- Two questions carried over from Lecture 24 . . . 13
- Antisymmetry . . . 16
- Worked: symmetric against antisymmetric . . . 17
- Comparable and non-comparable elements . . . 18
- Partial and total orders . . . 20
- Worked: "divides" is a partial order . . . 22
- Hasse diagrams . . . 23
- Worked: the Hasse diagram of a power set . . . 24
- See also . . . 24

Lecture 26 — Definitions and Examples of Groups **25**
- Goals . . . 25
- Modular arithmetic and the group $\mathbb{Z}_n$ . . . 26
- The definition of a group . . . 27

Worked: which of these are groups? . . . 27
Worked: a multiplication table mod 7 . . . 28
The symmetric group S_n . . . 29
Worked: the Cayley table of S_3 . . . 31
S_3 is a non-abelian group . . . 33
Worked: no repeats in a row . . . 36
See also . . . 36

Reference material **37**
Antisymmetric Relations . . . 37
Cayley Tables . . . 43
Composition of Functions . . . 49
Countable and Uncountable Sets . . . 54
Divisibility & Unique Factorisation . . . 60
Equivalence Classes and Partitions . . . 66
Equivalence Relations . . . 73
Groups . . . 80
Hasse Diagrams . . . 90
The Integers Modulo n . . . 94
Modular Arithmetic, Floor & the Quotient-Remainder Theorem . . . 101
One-to-One and Onto Functions . . . 107
Partial Order Relations . . . 112
Practice Problems — the Semester-wide Set . . . 118
Rational & Irrational Numbers . . . 243
Reflexive, Symmetric and Transitive Relations . . . 249
Sets and Set Notation . . . 254
The Symmetric Group . . . 266

Lecture 24 — Equivalence Relations

Equivalence relations, their classes, and why the classes cut the set into a partition. Prework: Video 031 (Equivalence Relations). The definition and how to prove or disprove it are collected in equivalence-relations[1], and classes, partitions and the two-way link between them in equivalence-classes-and-partitions[2]. The three properties come from reflexive-symmetric-and-transitive-relations[3].

[1] courses/math1061/equivalence-relations.pdf
[2] courses/math1061/equivalence-classes-and-partitions.pdf
[3] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf

Goals

1. Know how to prove or disprove that a relation is an **equivalence relation**.
2. Understand **equivalence classes**.
3. Understand the connection between equivalence relations and **partitions**.

All three in one sentence:

> If R is an equivalence relation on a set A, then the equivalence classes of R partition A.

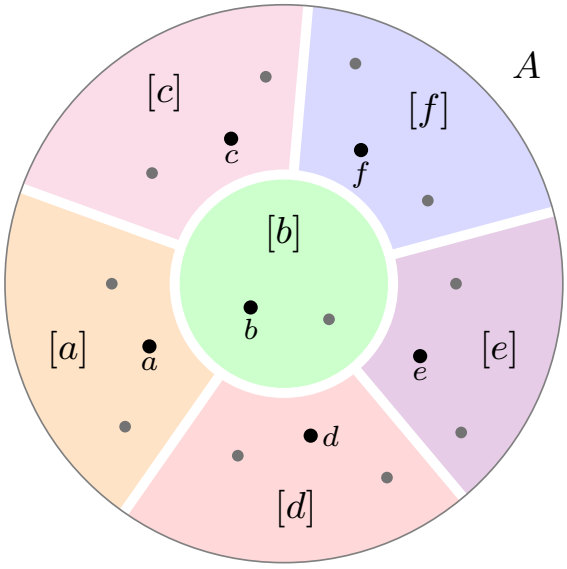


Figure 1: A set A cut into the equivalence classes of a relation on it. Every element of A lies in exactly one region. Each region is named after one of the elements in it, written in square brackets: $[a]$ is the region that a is in. The regions cover A and no two overlap, and that is what a partition is.

Three questions to start with

Are there any equivalence relations apart from congruence mod n and equality? Yes. Fractions are one. Take pairs of positive integers and relate

$$(a, b) \sim (c, d) \quad \text{if and only if} \quad ad = bc,$$

which is the condition $\frac{a}{b} = \frac{c}{d}$ written without division. Then $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots$ says that $(1, 2)$, $(2, 4)$ and $(3, 6)$ are all related: three pairs in one class. A positive rational number is a whole class of pairs. The relation is worked through in equivalence-relations[4].

What exactly is the equivalence class $[a]$? The set of everything related to a. See Equivalence classes.

Why does the set of equivalence classes form a partition, and given a partition, how do we get an equivalence relation? The first is Two classes are equal or disjoint, and the second is From a partition to an equivalence relation.

The definition

For a relation ρ on a set A (reflexive-symmetric-and-transitive-relations[5]):

Property	Condition
reflexive	$\forall x \in A,\ x\ \rho\ x$
symmetric	$\forall x, y \in A,\ x\ \rho\ y \to y\ \rho\ x$
transitive	$\forall x, y, z \in A,\ (x\ \rho\ y \text{ and } y\ \rho\ z) \to x\ \rho\ z$

A relation is an **equivalence relation** if and only if it is reflexive, symmetric and transitive.

Worked: the sum is rational

Let ρ be the relation on $\mathbb{R}$ defined by: for all $x, y \in \mathbb{R}$, $x\ \rho\ y$ if and only if $x + y \in \mathbb{Q}$. Is ρ an equivalence relation?

No. ρ is not reflexive.

Take $x = \sqrt{2} \in \mathbb{R}$. Then $x + x = \sqrt{2} + \sqrt{2} = 2\sqrt{2} \notin \mathbb{Q}$, so $\sqrt{2} \not\rho \sqrt{2}$. $\therefore \rho$ is not an equivalence relation.

Reflexive is a "for all" statement, $\forall x \in A,\ x\ \rho\ x$, so a single x that fails disproves it. An equivalence relation needs all three properties, so **one failed property, shown by one witness, settles the question**. There is no need to look at the other two.

For the record, ρ is symmetric, because $x + y = y + x$. It is not transitive: $\sqrt{2}\ \rho\ -\sqrt{2}$ and $-\sqrt{2}\ \rho\ \sqrt{2}$, since both sums are 0, but $\sqrt{2} \not\rho \sqrt{2}$. That is the forced loop of reflexive-symmetric-and-transitive-relations[6] again.

[4] courses/math1061/equivalence-relations.pdf
[5] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[6] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf

Worked: the difference is rational

> Let τ be the relation on $\mathbb{R}$ defined by: for all $x, y \in \mathbb{R}$, $x \tau y$ if and only if $x - y \in \mathbb{Q}$.
> Is τ an equivalence relation?

Yes. The proof has three parts, one for each property.

(1) Reflexive. Let $x \in \mathbb{R}$. *(Think: is $x \tau x$?)* $x - x = 0 \in \mathbb{Q}$, since $0 = \frac{0}{1}$. So τ is reflexive.

(2) Symmetric. Let $x, y \in \mathbb{R}$ and suppose $x \tau y$. Then $x - y \in \mathbb{Q}$, so $x - y = \dfrac{a}{b}$ for some $a, b \in \mathbb{Z}$, $b \neq 0$.

$$y - x = -(x - y) = -\left(\frac{a}{b}\right) = \frac{-a}{b}.$$

Since $-a \in \mathbb{Z}$ we have $y - x \in \mathbb{Q}$, so $y \tau x$. $\therefore \tau$ is symmetric.

(3) Transitive. Let $x, y, z \in \mathbb{R}$ and suppose $x \tau y$ and $y \tau z$. Thus $x - y = \dfrac{a}{b}$ and $y - z = \dfrac{c}{d}$ for some $a, b, c, d \in \mathbb{Z}$, $b \neq 0$, $d \neq 0$.

$$\text{Now } x - z = (x - y) + (y - z) = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Since $a, b, c, d \in \mathbb{Z}$, $ad + bc$, $bd \in \mathbb{Z}$. Also $bd \neq 0$. $\therefore x - z \in \mathbb{Q}$, so $x \tau z$. $\therefore \tau$ is transitive.

Three things to copy from this proof:

- **Start each part by asking what the property says for this relation.** For reflexive that is "is $x \tau x$?", which is "is $x - x \in \mathbb{Q}$?".
- **Each part unfolds the definition.** "$x - y \in \mathbb{Q}$" is turned into $x - y = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$ (rational-and-irrational-numbers[7]), worked on, and folded back up into "$\in \mathbb{Q}$".
- **New letters for the second fraction.** Part (3) uses $\frac{c}{d}$ for $y - z$. Writing $\frac{a}{b}$ again would claim the two differences are equal.

The step that makes part (3) work is $x - z = (x - y) + (y - z)$: the middle term cancels. For sums there is no such identity, which is where ρ goes wrong.

Partitions

> Two sets X and Y are **disjoint** if and only if $X \cap Y = \emptyset$.
> A collection of sets is **mutually disjoint** if each pair of distinct sets in the collection is disjoint.

> A **partition** of a set S is a collection of non-empty and mutually disjoint subsets of S whose union is S.
> The subsets in a partition are sometimes called **parts**.

[7] courses/math1061/rational-and-irrational-numbers.pdf

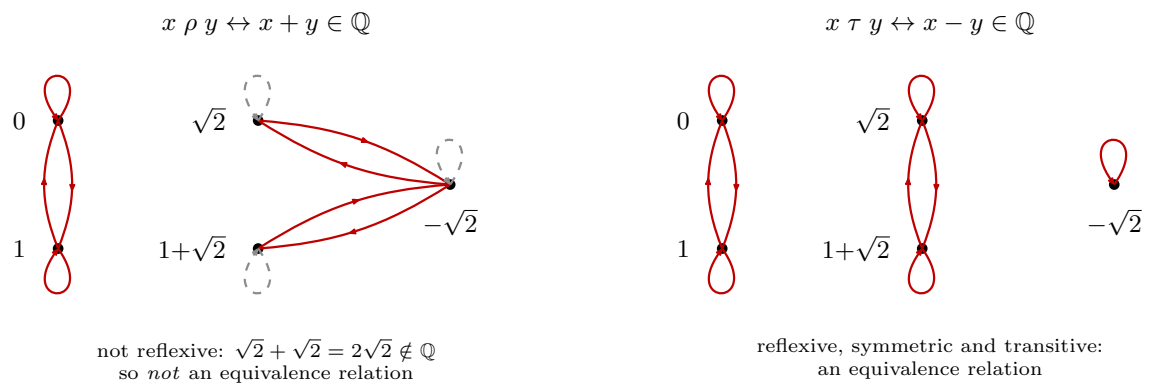


Figure 2: The same five real numbers under the two relations. Left, $x \rho y \leftrightarrow x + y \in \mathbb{Q}$. Only 0 and 1 have loops. There is none at $\sqrt{2}$ because $\sqrt{2} + \sqrt{2}$ is irrational, so ρ is not reflexive, and the three missing loops are dashed. Right, $x \tau y \leftrightarrow x - y \in \mathbb{Q}$. Every number has a loop because $x - x = 0$, and the numbers fall into three separate clusters with every arrow present inside a cluster and none between clusters. That clustered shape is what an equivalence relation looks like.

This is the definition from sets-and-set-notation[8] with two new words, *mutually disjoint* and *parts*. Three conditions: the pieces are non-empty, no two overlap, and together they cover S.

The positive integers by remainder.

$$\{\{1, 4, 7, \dots\},\ \{2, 5, 8, \dots\},\ \{3, 6, 9, \dots\}\} \text{ is a partition of } \mathbb{Z}^+.$$

The three parts are the positive integers sorted by remainder on division by 3. A partition is always a partition *of* some set, here $\mathbb{Z}^+$, and naming that set is part of the statement.

One set, two partitions. Let $S = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9\}$.

- $\{\{x_1, x_2, x_3\},\ \{x_4, x_5\},\ \{x_6, x_7, x_8, x_9\}\}$ is a partition of S with 3 parts.
- $\{\{x_1, x_2\},\ \{x_3, x_4\},\ \{x_5, x_8, x_9\},\ \{x_6, x_7\}\}$ is another partition of S, with 4 parts.

One set has many partitions. The parts need not be the same size, and their elements need not be next to each other in any listing: $\{x_5, x_8, x_9\}$ is a part.

Mutually disjoint, and not. Let $W = \{1, 2, 3\}$, $X = \{4, 5, 6\}$, $Y = \{6, 7, 8\}$, $Z = \{7, 8, 9, 10\}$.

- W, X and Z are mutually disjoint.

[8] courses/math1061/sets-and-set-notation.pdf

- W, X and Y are **not** mutually disjoint, because $X \cap Y = \{6\}$. One overlapping pair is enough, even though W is disjoint from both of the others.
- $\{W, X, Z\}$ is a partition of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ with 3 parts.

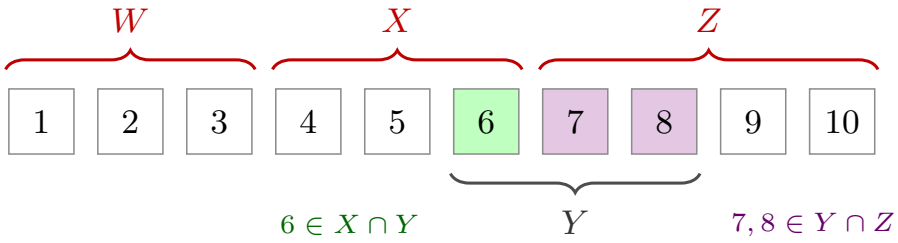


Figure 3: The four sets W, X, Y and Z on the numbers 1 to 10. W, X and Z sit side by side and share no number, so they are mutually disjoint, and between them they use every number from 1 to 10, so W, X, Z is a partition with three parts. Y shares 6 with X and shares 7 and 8 with Z. A collection that contains Y together with X or Z is not mutually disjoint, however many of its other pairs are disjoint. The shared numbers are shaded, 6 in green and 7 and 8 in purple.

Equivalence classes

Let ρ be an equivalence relation on a set S. For each $a \in S$, the **equivalence class** of a is

$$[a] = \{x \in S : x \ \rho \ a\},$$

the set of elements related to a.

The equivalence classes of an equivalence relation on a set S form a partition of S.

Congruence mod 3. For $m \ T \ n \leftrightarrow m \equiv n \pmod 3$ on $\mathbb{Z}$ there are three classes:

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\}, \qquad [1] = \{\dots, -5, -2, 1, 4, 7, \dots\}, \qquad [2] = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

Also $[0] = [3] = [-6]$. A class is a set, and the bracket only says which element was used to name it. Every element of a class names that same class, so a class with infinitely many elements has infinitely many names.

Same parity. The relation ρ on $\mathbb{Z}$ defined by "$m \ \rho \ n$ if and only if m and n have the same parity" is an equivalence relation. Its equivalence classes are

$$\mathbb{Z}^{even} = \{\dots, -4, -2, 0, 2, 4, \dots\} \qquad \text{and} \qquad \mathbb{Z}^{odd} = \{\dots, -3, -1, 1, 3, 5, \dots\},$$

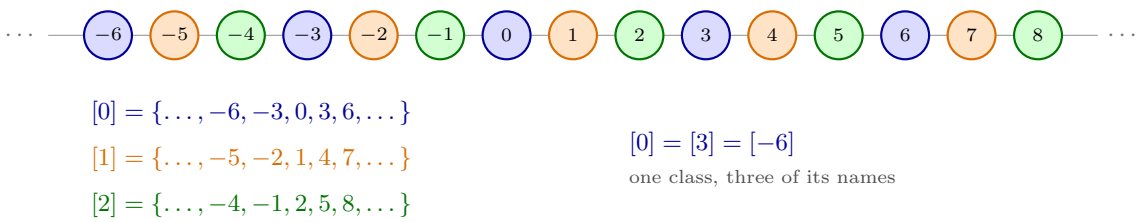


Figure 4: The integers from −6 to 8, coloured by remainder on division by 3. Each colour is one equivalence class of $m \equiv n \pmod 3$. The classes are spread along the number line, every third integer, and each integer has exactly one colour, so the three classes partition $\mathbb{Z}$. The line at the right gives one class three of its names: [0], [3] and [−6] are the same set, named after three different elements of it.

and these two classes partition $\mathbb{Z}$.

As an arrow diagram, the inside of a class has a loop at every element and arrows both ways between every pair. All of its elements are related to each other and to themselves, and none is related to anything outside.

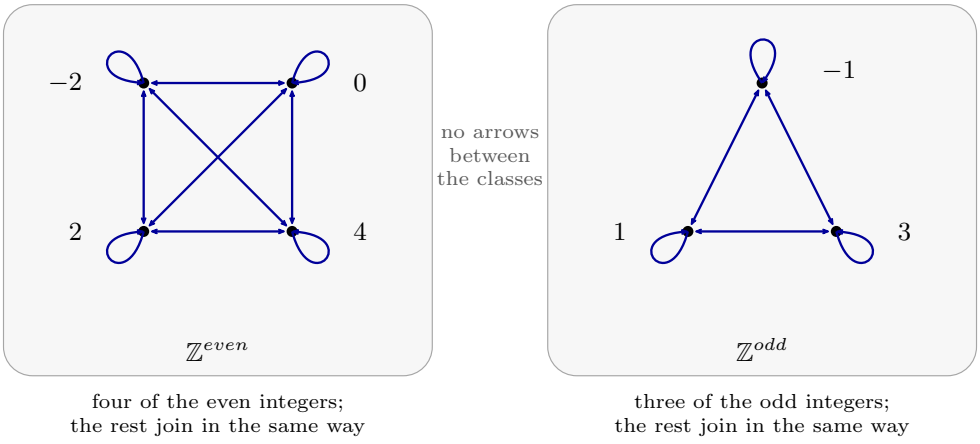


Figure 5: Inside one equivalence class every element is related to every other, in both directions, and to itself. Between two different classes there are no arrows at all. Shown for the relation *same parity* on $\mathbb{Z}$, with four of the even integers and three of the odd ones. Each double-headed line stands for one arrow each way.

Worked: the classes of τ

τ is the equivalence relation from before: for all $x, y \in \mathbb{R}$, $x \,\tau\, y$ if and only if $x - y \in \mathbb{Q}$.

(a) Describe the equivalence class $[1]$.

$$1 \tau y \;\leftrightarrow\; 1 - y \in \mathbb{Q} \;\leftrightarrow\; y \in \mathbb{Q}, \qquad \text{so} \qquad [1] = \mathbb{Q}.$$

The method is to ask which y are related to 1 and unfold the definition until it is a plain condition on y. The class is defined as the x with $x \tau 1$, and this works with $1 \tau y$ instead. For an equivalence relation the order makes no difference, because it is symmetric.

(b) State three elements that are in the equivalence class $[\sqrt{2}]$.

- $\sqrt{2} \in [\sqrt{2}]$, because $\sqrt{2} - \sqrt{2} = 0 \in \mathbb{Q}$, so $\sqrt{2} \tau \sqrt{2}$.
- $1 + \sqrt{2} \in [\sqrt{2}]$, because $\sqrt{2} - (1 + \sqrt{2}) = -1 \in \mathbb{Q}$.
- $-3 + \sqrt{2} \in [\sqrt{2}]$, because $\sqrt{2} - (-3 + \sqrt{2}) = 3 \in \mathbb{Q}$.

The whole class is

$$[\sqrt{2}] = \{y + \sqrt{2} : y \in \mathbb{Q}\}.$$

The first element is the standard one. a **is always in** $[a]$, because the relation is reflexive.

(c) Is $[\sqrt{2}] = [-\sqrt{2}]$?

$\sqrt{2} - (-\sqrt{2}) = 2\sqrt{2} \notin \mathbb{Q}$, so $\sqrt{2} \not\tau -\sqrt{2}$. Therefore $[\sqrt{2}] \neq [-\sqrt{2}]$.

To compare two classes, test their two names against each other. Related names give the same class, and unrelated names give different classes. Why that is enough is the next section.

So $\mathbb{R}$ is cut into classes, of which $[1] = \mathbb{Q}$, $[\sqrt{2}]$ and $[-\sqrt{2}]$ are three.

Each class of τ is a copy of $\mathbb{Q}$, so it is countable, and $\mathbb{R}$ is not (countable-and-uncountable-sets[9]). So there are infinitely many classes besides these three.

Two classes are equal or disjoint

> **True or false:** if the equivalence class $[a]$ is equal to the equivalence class $[b]$, then $b \in [a]$.

True. $b \in [b]$ because the relation is reflexive. So if $[a] = [b]$ then

$$b \in [b] = [a].$$

The result behind it:

[9] courses/math1061/countable-and-uncountable-sets.pdf

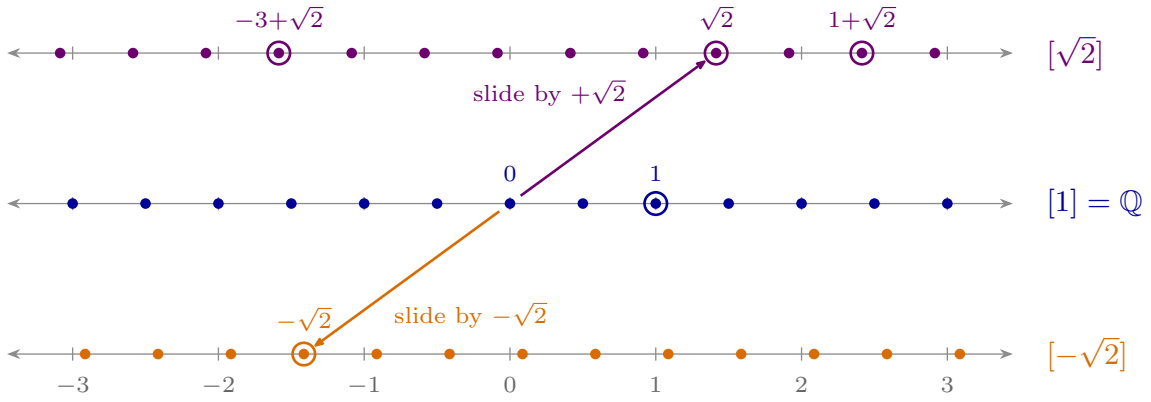


Figure 6: Three of the equivalence classes of τ, each on its own copy of the real line. A class cannot be drawn in full, so only the numbers a multiple of $\frac{1}{2}$ away from the class's name are shown. $[1]$ is $\mathbb{Q}$. $[\sqrt{2}] = y + \sqrt{2} : y \in \mathbb{Q}$ is $\mathbb{Q}$ slid $\sqrt{2}$ to the right, and $[-\sqrt{2}]$ is $\mathbb{Q}$ slid $\sqrt{2}$ to the left. The ringed points are 1, the three elements found for $[\sqrt{2}]$, and $-\sqrt{2}$. No point of one line is directly above a point of another, since a real number is in only one class.

Important result. If ρ is an equivalence relation on a set S, and $a, b \in S$, then either

$$[a] = [b] \qquad \text{or} \qquad [a] \cap [b] = \emptyset.$$

If $a \;\rho\; b$ the classes are equal, and if $a \not\rho\; b$ they are disjoint.

Two classes are either the same set or have nothing in common. They never partly overlap.

This is why the equivalence classes form a partition:

- the classes are non-empty, since $a \in [a]$;
- every element is in a class, its own, so their union is S;
- two different classes are disjoint, by the result.

The proof of the result, with a picture, is in equivalence-classes-and-partitions[10].

Worked: a relation defined with "or"

The relation σ on $\mathbb{Z}$ is defined by $m \;\sigma\; n \leftrightarrow$ (8 divides $m - n$) or (8 divides $m + n$). It is an equivalence relation. Describe its equivalence classes.

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

The proof that it is an equivalence relation is below. The classes are worked out in 2026-09-22-partial-order-relations[11]: there are five of them.

Proof that σ is an equivalence relation

Reflexive. Let $m \in \mathbb{Z}$. Then $m - m = 0$ and 8 divides 0, so $8 \mid (m - m)$, hence $m \sigma m$. Thus σ is reflexive.

Symmetric. Let $m, n \in \mathbb{Z}$ and suppose $m \sigma n$. So $8 \mid (m - n)$ or $8 \mid (m + n)$.

- Case 1: Suppose $8 \mid (m - n)$. Note that $n - m = -(m - n)$, and if an integer is divisible by 8 then its negative is divisible by 8. Hence $8 \mid (n - m)$. Hence $n \sigma m$.
- Case 2: Suppose $8 \mid (m + n)$. Then $8 \mid (n + m)$ since addition is commutative. Hence $n \sigma m$.

Thus σ is symmetric.

Transitive. Let $k, m, n \in \mathbb{Z}$ and suppose $k \sigma m$ and $m \sigma n$. Thus $8 \mid (k - m)$ or $8 \mid (k + m)$. Also $8 \mid (m - n)$ or $8 \mid (m + n)$.

- Case 1: $8 \mid (k - m)$ and $8 \mid (m - n)$. Then $8 \mid ((k - m) + (m - n))$ so $8 \mid (k - n)$. Hence $k \sigma n$.
- Case 2: $8 \mid (k - m)$ and $8 \mid (m + n)$. Then $8 \mid ((k - m) + (m + n))$ so $8 \mid (k + n)$. Hence $k \sigma n$.
- Case 3: $8 \mid (k + m)$ and $8 \mid (m - n)$. Then $8 \mid ((k + m) - (m - n))$ so $8 \mid (k + n)$. Hence $k \sigma n$.
- Case 4: $8 \mid (k + m)$ and $8 \mid (m + n)$. Then $8 \mid ((k + m) - (m + n))$ so $8 \mid (k - n)$. Hence $k \sigma n$.

Thus σ is transitive. Therefore σ is an equivalence relation. ■

How the proof is organised:

- The definition of σ is an *or*, so a hypothesis $m \sigma n$ splits into two cases, and two such hypotheses split into $2 \times 2 = 4$.
- In each transitivity case the two divisible quantities are **added or subtracted, whichever cancels the** m: cases 1 and 2 add, cases 3 and 4 subtract. What is left is $k - n$ or $k + n$, and either one gives $k \sigma n$.
- It uses that a sum or difference of two multiples of 8 is a multiple of 8 (divisibility-and-factorisation[12]).

[11] courses/math1061/2026-09-22-partial-order-relations.pdf
[12] courses/math1061/divisibility-and-factorisation.pdf

From a partition to an equivalence relation

The link also runs the other way.

> Given any partition of a set S, we can define an equivalence relation on S by taking two elements to be related if and only if they are in the same part of the partition. The parts of the partition are then the equivalence classes of that relation.
>
> **Any partition defines an equivalence relation, and any equivalence relation defines a partition.**

Example. Let $S = \{1, 2, 3, 4, 5, 6\}$ with the partition $\{\{1, 2, 3\}, \{4, 5\}, \{6\}\}$. The equivalence relation R on S built from this partition is

$$R = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4), (4,5), (5,5), (5,4), (6,6)\}.$$

R has three equivalence classes:

$$[1] = \{1, 2, 3\} = [2] = [3], \qquad [4] = \{4, 5\} = [5], \qquad [6] = \{6\}.$$

A part with k elements contributes all $k \times k$ pairs of its elements, loops included, so R has $3^2 + 2^2 + 1^2 = 14$ pairs. Reading the classes back off R returns the partition it was built from.

> **Question.** Consider the partition of the integers given by $\{\mathbb{Z}^-, \{0\}, \mathbb{Z}^+\}$. Describe an equivalence relation that corresponds to this partition.

Answered in 2026-09-22-partial-order-relations[13].

See also

- equivalence-relations[14] — the definition, the proof template, and these relations side by side
- equivalence-classes-and-partitions[15] — classes, why two classes are equal or disjoint, and partitions to relations and back
- reflexive-symmetric-and-transitive-relations[16] — the three properties an equivalence relation needs
- sets-and-set-notation[17] — partitions as first defined

[13] courses/math1061/2026-09-22-partial-order-relations.pdf
[14] courses/math1061/equivalence-relations.pdf
[15] courses/math1061/equivalence-classes-and-partitions.pdf
[16] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[17] courses/math1061/sets-and-set-notation.pdf

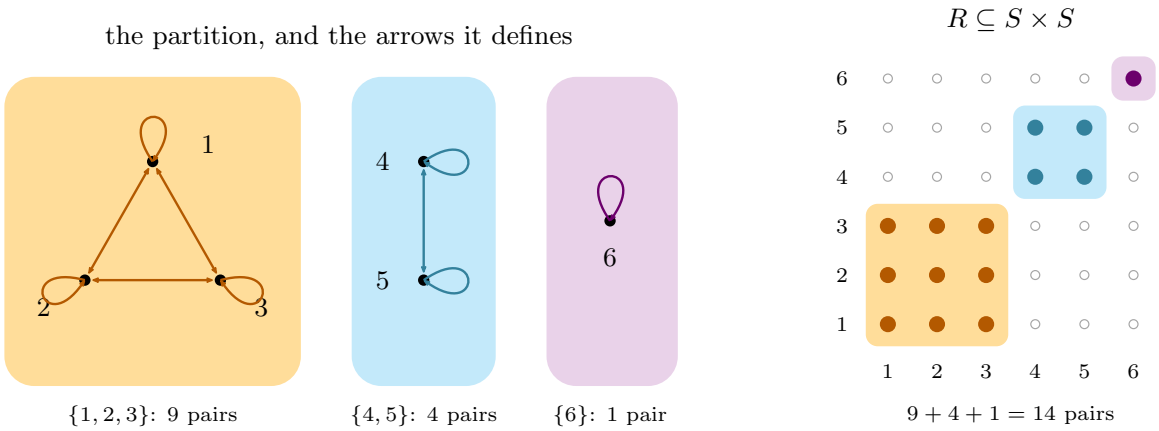


Figure 7: From a partition to the relation it defines. Left: the three parts of $S = 1, \dots, 6$, and inside each part every arrow, since two elements are related exactly when they are in the same part. Right: the same relation as a set of points in the grid $S \times S$, the first coordinate across and the second up. Each part gives a solid square block on the diagonal, 3×3, 2×2 and 1×1, so R has $9 + 4 + 1 = 14$ pairs. Yellow marks $1, 2, 3$ and its nine pairs, cyan $4, 5$ and its four, purple 6 and $(6, 6)$.

- modular-arithmetic[18] — congruence, the standard source of equivalence relations
- 2026-09-17-relations-reflexivity-symmetry-transitivity[19] — Lecture 23 · 2026-09-22-partial-order-relations[20] — Lecture 25
- practice-problems[21] — §31, with full worked solutions

Lecture 25 — Partial Order Relations

Antisymmetry, comparable elements, partial and total orders, and Hasse diagrams. Pre-work: Video 032 (Partial Order Relations). The new property is collected in antisymmetric-relations[22], comparable elements and the two kinds of order in partial-order-relations[23], and the simplified drawing in hasse-diagrams[24]. The note starts with two questions left over from 2026-09-21-equivalence-relations[25].

[18] courses/math1061/modular-arithmetic.pdf
[19] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf
[20] courses/math1061/2026-09-22-partial-order-relations.pdf
[21] courses/math1061/practice-problems.pdf
[22] courses/math1061/antisymmetric-relations.pdf
[23] courses/math1061/partial-order-relations.pdf
[24] courses/math1061/hasse-diagrams.pdf
[25] courses/math1061/2026-09-21-equivalence-relations.pdf

Goals

1. Understand **antisymmetry**, **comparable**, **partial order**, **total order** in the context of relations.
2. Learn how to prove a relation is **antisymmetric**.
3. Learn how to prove a relation is a **partial/total order**.
4. Learn how to draw a **Hasse diagram**.

Two things to have straight before starting:

- **Antisymmetric does not mean "not symmetric".** A relation can be both, either one, or neither. Symmetric against antisymmetric has one of each.
- $2 \mid 6$ **is a statement.** "2 divides 6" is true or false. It is not a number, and in particular it is not the fraction $\frac{2}{6}$ (divisibility-and-factorisation[26]). The relation "divides" is the subject of a worked proof below.

Two questions carried over from Lecture 24

The classes of σ

> The relation σ on $\mathbb{Z}$ defined by $m \,\sigma\, n \leftrightarrow$ (8 divides $m-n$) or (8 divides $m+n$) is an equivalence relation. Describe the equivalence classes of σ.

Work out one class at a time, starting from the definition of a class:

$$\begin{aligned}
[1] &= \{n \in \mathbb{Z} : 8 \mid (1-n) \text{ or } 8 \mid (1+n)\} \\
&= \{n \in \mathbb{Z} : n \equiv 1 \text{ or } 7 \pmod 8\} && = [7] \\
[2] &= \{n \in \mathbb{Z} : 8 \mid (2-n) \text{ or } 8 \mid (2+n)\} \\
&= \{n \in \mathbb{Z} : n \equiv 2 \text{ or } 6 \pmod 8\} && = [6] \\
[3] &= \{n \in \mathbb{Z} : n \equiv 3 \text{ or } 5 \pmod 8\} && = [5] \\
[4] &= \{n \in \mathbb{Z} : 8 \mid (4-n) \text{ or } 8 \mid (4+n)\} \\
&= \{n \in \mathbb{Z} : n \equiv 4 \pmod 8\} \\
[0] &= \{n \in \mathbb{Z} : n \equiv 0 \pmod 8\}
\end{aligned}$$

For example 1, 9, 7 and 17 are four elements of [1].

So σ has **five** classes. The reason:

[26] courses/math1061/divisibility-and-factorisation.pdf

- $8 \mid (a - n)$ says $n \equiv a \pmod 8$, and $8 \mid (a + n)$ says $n \equiv -a \pmod 8$. So $[a]$ collects the integers congruent to a together with the integers congruent to $-a$.
- Mod 8, $-1 \equiv 7$, $-2 \equiv 6$ and $-3 \equiv 5$, which joins the remainders in pairs.
- But $-4 \equiv 4$ and $-0 \equiv 0$, so $[4]$ and $[0]$ get nothing extra.

Every integer has exactly one remainder from 0 to 7, so every integer is in exactly one of the five classes, as it must be.

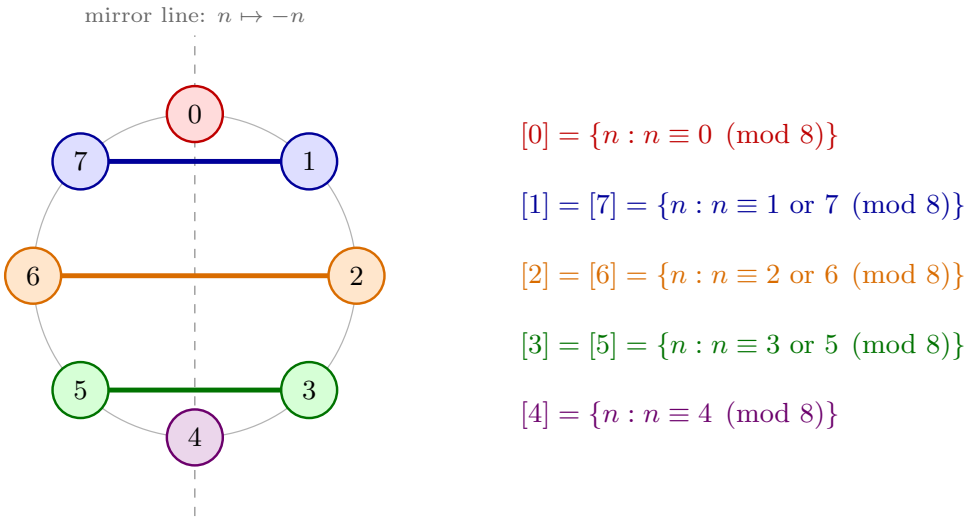


Figure 8: The eight remainders mod 8 on a clock face. Congruence mod 8 on its own has eight classes, one for each remainder. The relation σ also relates n to everything congruent to $-n$, and replacing a remainder by its negative is the left-to-right flip of the clock. So each remainder is joined to its mirror image: 1 with 7, 2 with 6, 3 with 5. The remainders 0 and 4 lie on the mirror line and are their own images. That leaves five classes.

The proof that σ is an equivalence relation is in 2026-09-21-equivalence-relations[27].

A relation for the partition by sign

Any partition defines an equivalence relation: two elements are related if and only if they are in the same part (2026-09-21-equivalence-relations[28]).

> Consider the partition of the integers given by $\{\mathbb{Z}^-, \{0\}, \mathbb{Z}^+\}$. Describe an equivalence relation that corresponds to this partition.

[27] courses/math1061/2026-09-21-equivalence-relations.pdf
[28] courses/math1061/2026-09-21-equivalence-relations.pdf

Define τ by: for all $a, b \in \mathbb{Z}$,

$$a \,\tau\, b \iff a, b \text{ both positive} \quad \text{or} \quad a = b = 0 \quad \text{or} \quad a, b \text{ both negative.}$$

The condition has one alternative for each part. The middle part has one element, so "both in $\{0\}$" becomes $a = b = 0$.

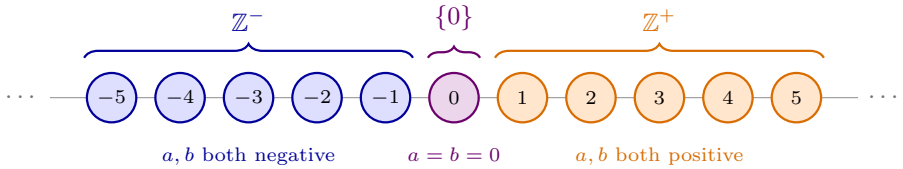


Figure 9: The partition $\mathbb{Z}^-, 0, \mathbb{Z}^+$ of the integers, shown from -5 to 5, and the relation it defines. Two integers are related exactly when they have the same colour. So $-4 \,\tau\, -1$ and $2 \,\tau\, 5$, the only thing related to 0 is 0, and no negative integer is related to a positive one.

Antisymmetry

Definition. A relation R on a set S is **antisymmetric** if and only if

$$\forall a, b \in S,\ (a \ R\ b \text{ and } b \ R\ a) \to (a = b).$$

There are two equivalent ways to write it:

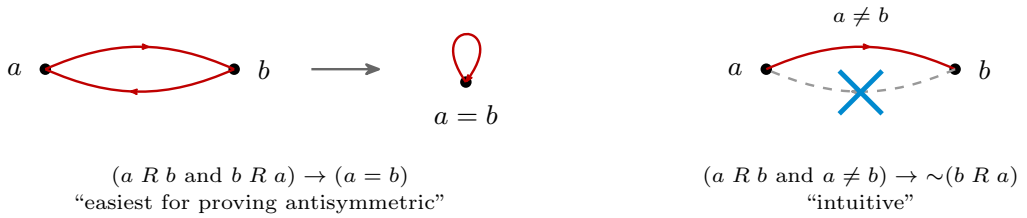
$$\forall a, b \in S,\ (a \neq b) \to \sim(a \ R\ b \text{ and } b \ R\ a)$$

$$\forall a, b \in S,\ (a \ R\ b \text{ and } a \neq b) \to \sim(b \ R\ a)$$

The first form is the **easiest for proving** a relation antisymmetric. The third is the most **intuitive**.

All three say the same thing about the arrow diagram: **there is no pair of different elements with arrows both ways**.

- The first reads it as "if you do find arrows both ways, the two ends were the same element all along", so the pair of arrows is really one loop.
- The third reads it as "an arrow from a to a different element b has no return".
- Loops are not restricted at all.



$(a\ R\ b \text{ and } b\ R\ a) \to (a = b)$
"easiest for proving antisymmetric"

$(a\ R\ b \text{ and } a \neq b) \to \sim(b\ R\ a)$
"intuitive"

Figure 10: Antisymmetry in two pictures. Left, the first definition: arrows both ways between a and b are only possible if a and b are the same element, in which case the picture is a single dot with a loop. This is the form to use in a proof. Right, the third definition: an arrow from a to a different element b rules out the arrow back from b to a. This is the form to picture.

Examples.

- $\leq$ on $\mathbb{R}$ is antisymmetric: for all $x, y \in \mathbb{R}$, $(x \leq y \text{ and } y \leq x) \to (x = y)$.
- So are $<$, $>$ and $\geq$ on $\mathbb{R}$.
- "Divides" is antisymmetric on $\mathbb{Z}^+$. It is proved below.
- $\subseteq$ on any set S of sets is antisymmetric: for all $X, Y \in S$, $(X \subseteq Y \text{ and } Y \subseteq X) \to (X = Y)$. This is the double-containment rule for showing two sets are equal (sets-and-set-notation[29]).

Why $<$ counts, and why "divides" needs $\mathbb{Z}^+$ and not $\mathbb{Z}$, are in antisymmetric-relations[30].

Worked: symmetric against antisymmetric

Symmetric says every arrow has a return: $\forall a, b \in A,\ a\ \rho\ b \to b\ \rho\ a$. Antisymmetric says no arrow between different elements has one: $\forall a, b \in S,\ (a\ R\ b \text{ and } b\ R\ a) \to (a = b)$.

Match each of the four arrow diagrams with the description of its relation.

A. Both symmetric and antisymmetric
B. Symmetric but not antisymmetric
C. Antisymmetric but not symmetric
D. Neither symmetric nor antisymmetric

Each diagram has three dots.

[29] courses/math1061/sets-and-set-notation.pdf
[30] courses/math1061/antisymmetric-relations.pdf

	The arrows	Answer	Why
Diagram 1	both ways between the first and second dots; one arrow from the second to the third; a loop at the third	**D**	the two-way pair joins different elements, so not antisymmetric; the single arrow has no return, so not symmetric
Diagram 2	a loop at each of two dots; the third dot has no arrows	**A**	the only arrows are loops, which break neither property
Diagram 3	both ways between the first and second dots, and both ways between the second and third; a loop at the third	**B**	every arrow has a return, so symmetric; the two-way pairs join different elements, so not antisymmetric
Diagram 4	one arrow from the first dot to the second, and one from the second to the third; a loop at the third	**C**	neither single arrow has a return, so not symmetric; there is no two-way pair, so antisymmetric

Diagram 2 is the one that shows antisymmetric is not the opposite of symmetric. Its only arrows are loops. A loop is its own return, so the relation is symmetric. There are no arrows between different elements, so nothing can break antisymmetry.

Comparable and non-comparable elements

> If R is a relation on a set S, then two elements $a, b \in S$ are **comparable** if and only if $a \; R \; b$ or $b \; R \; a$.

Comparable means **related in some direction**.

Example. A relation R on six points a to f, with arrows $a \to c$ and $c \to a$, $c \to e$, $b \to a$, $b \to e$, $f \to b$, $b \to d$, and loops at b and at e:

Comparable	Noncomparable
a and c	a and e
a and b	a and d

Comparable	Noncomparable
c and e	a and f
b and e	b and c
b and d	c and d
b and f	c and f
	d and e
b and b	d and f
e and e	e and f

What the two columns show:

- **Direction does not matter.** a and b are comparable because of the arrow $b \to a$. One arrow either way is enough.
- **Comparable means one arrow, not a path.** a and e are noncomparable although $a \to c \to e$ is a path, because there is no arrow between them. This R is not transitive.
- **An element is comparable with itself only if it has a loop.** Only b and e are comparable with themselves.
- The 15 pairs of different points split 6 and 9.

This R is not a partial order: a and c are joined both ways, and four points have no loop. The definition of comparable does not need one.

Worked: comparable sets

In the partial order relation defined on the power set $\mathcal{P}(\mathbb{Z})$ of $\mathbb{Z}$ by $X \rho Y$ iff $X \subseteq Y$, which of the following are comparable elements?

		Answer	Why
(a)	7 and 9	**not elements of** $\mathcal{P}(\mathbb{Z})$	7 and 9 are integers, not sets of integers, so the relation is not defined on them
(b)	$\{7\}$ and $\{9\}$	**non-comparable**	neither is a subset of the other
(c)	$\{7\}$ and $\{7, 9\}$	**comparable**	$\{7\} \subseteq \{7, 9\}$
(d)	$\{1, 2, 3\}$ and $\{1, 2, 4\}$	**non-comparable**	$3 \notin \{1, 2, 4\}$ and $4 \notin \{1, 2, 3\}$, so neither contains the other

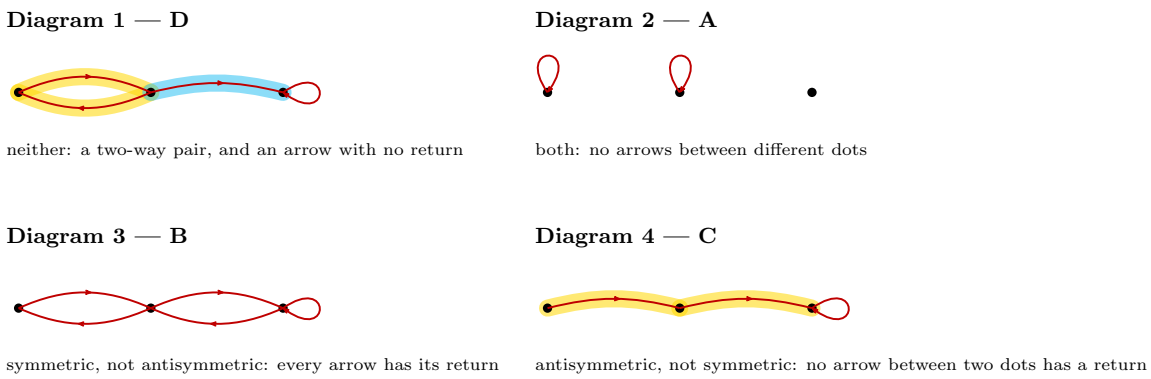


Figure 11: Four relations on three points, with their answers. Between two different dots there are three possibilities: no arrow, one arrow, or arrows both ways. A single arrow breaks symmetry, and arrows both ways break antisymmetry. Diagram 1 has one of each, the single arrow shaded cyan and the two-way pair yellow, so it is neither. Diagram 2 has no arrows between different dots, so it is both. Diagram 3 has only two-way pairs, so it is symmetric and not antisymmetric. Diagram 4 has only single arrows, so it is antisymmetric and not symmetric. The loops play no part in any of the four answers.

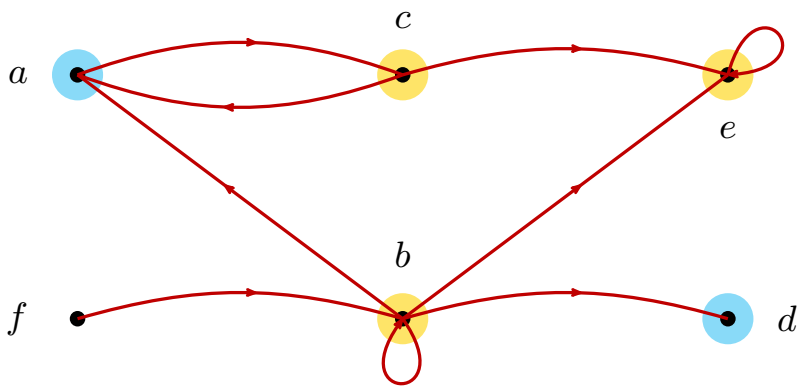


Figure 12: The relation R on six points, with three pairs highlighted. c and e, in yellow, are comparable: there is an arrow $c \to e$. b is comparable with itself, since it has a loop. a and d, in cyan, are not comparable: no arrow joins them in either direction. Two points are comparable when at least one arrow joins them, whichever way it points.

So the answer is **(c)**. Two traps:

- In (a), the elements of $\mathcal{P}(\mathbb{Z})$ are *sets* of integers. That is the element-versus-subset distinction of sets-and-set-notation[31].
- In (d), the two sets overlap in $\{1, 2\}$. Overlapping is not being comparable.

Partial and total orders

A relation R on a set S is a **partial order relation** if and only if R is

1. reflexive;
2. antisymmetric; and
3. transitive.

A relation R on a set S is a **total order relation** if and only if R is

1. reflexive;
2. antisymmetric;
3. transitive; and
4. any two elements of S are comparable.

A total order is a partial order plus condition 4. So:

- Any total order relation is a partial order relation.
- A partial order relation is a total order relation **if and only if** every two elements are comparable.

As arrow diagrams, a total order is a single column: a loop at each element and an arrow from each element to every element above it. A partial order that is not total has at least one pair of elements with no arrow between them.

Worked: "divides" is a partial order

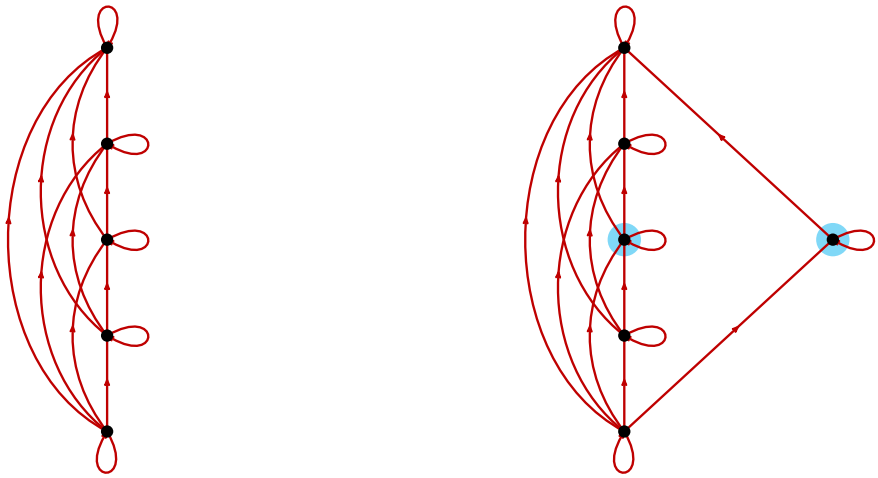
(a) Prove that the relation "divides" on $\mathbb{Z}^+$ is a partial order relation.
(b) Is the relation "divides" on $\mathbb{Z}^+$ a total order relation?

Name the relation and unfold it: for all $a, b \in \mathbb{Z}^+$,

$$a \tau b \leftrightarrow a \mid b \qquad \text{(that is, } b = ak \text{ for some } k \in \mathbb{Z}\text{)}.$$

(a)

[31] courses/math1061/sets-and-set-notation.pdf



a total order

a partial order that is
not a total order

Figure 13: Two orders as arrow diagrams. Left, a total order on five elements: a loop at each, and an arrow from each element to every element above it, ten in all. Every two elements are joined by an arrow, so every two are comparable. Right, a partial order that is not total: the same column and a sixth element off to the side, above the bottom element and below the top one. It is joined to nothing else in the column. The two elements shaded cyan are one of the three pairs that are not comparable.

Reflexive. Let $a \in \mathbb{Z}^+$. Since $a = a \cdot 1$ we have $a \mid a$, so τ is reflexive.

Antisymmetric. Let $a, b \in \mathbb{Z}^+$ and suppose $a \tau b$ and $b \tau a$. *(Goal: show $a = b$.)* Thus $b = ak$ for some $k \in \mathbb{Z}$ and $a = b\ell$ for some $\ell \in \mathbb{Z}$.

$$\text{Now } b = ak = (b\ell)k = b(\ell k), \qquad \text{so} \qquad 1 = \ell k.$$

(The b can be cancelled because $b \in \mathbb{Z}^+$, so $b \neq 0$.) Note $\ell > 0$ and $k > 0$ since $a, b > 0$. Thus $\ell = k = 1$, so $a = b$. $\therefore \tau$ is antisymmetric.

Transitive. Let $a, b, c \in \mathbb{Z}^+$ and suppose $a \tau b$ and $b \tau c$. Thus $b = ak$ and $c = b\ell$ for some $k, \ell \in \mathbb{Z}$. Hence $c = (ak)\ell = a(k\ell)$. Since $k\ell \in \mathbb{Z}$ we have $a \mid c$, that is, $a \tau c$. So τ is transitive.

$\therefore \tau$ is a partial order.

(b) Not a total order, since $2 \not\tau 3$ and $3 \not\tau 2$.

Points to notice:

- **State the goal.** The antisymmetric part begins by writing down where the first form of the definition is heading: show $a = b$.
- **Where $\mathbb{Z}^+$ is needed.** The step from $\ell k = 1$ to $\ell = k = 1$ uses that both are positive. On all of $\mathbb{Z}$, $\ell = k = -1$ is also possible, and the proof fails (antisymmetric-relations[32]).
- **One pair is enough for (b).** $2 \nmid 3$ and $3 \nmid 2$, so 2 and 3 are not comparable. "Any two elements are comparable" is a "for all", and one pair that fails disproves it.
- **The set matters.** On $\{1, 2, 4, 8, 16\}$ each number divides the next, every two are comparable, and "divides" is a total order there.

Hasse diagrams

A **Hasse diagram** for a partial order relation is obtained from its arrow diagram by:

1. placing the elements so that all the arrows point upwards;
2. deleting the loops (the arrows from elements to themselves);
3. deleting the arrows which are implied by the transitive property;
4. deleting the direction indicators on the arrows.

A Hasse diagram is sufficient to define a partial order relation.

Example. The six-element partial order of Figure 13, with the column named a, b, c, d, e from the bottom and f at the side. The arrow $a \to c$ is implied by $a \to b$ and $b \to c$, so it is one that step 3 deletes. What is left at the end is a, b, c, d, e in a vertical line joined by four segments, and f joined to a and to e.

[32] courses/math1061/antisymmetric-relations.pdf

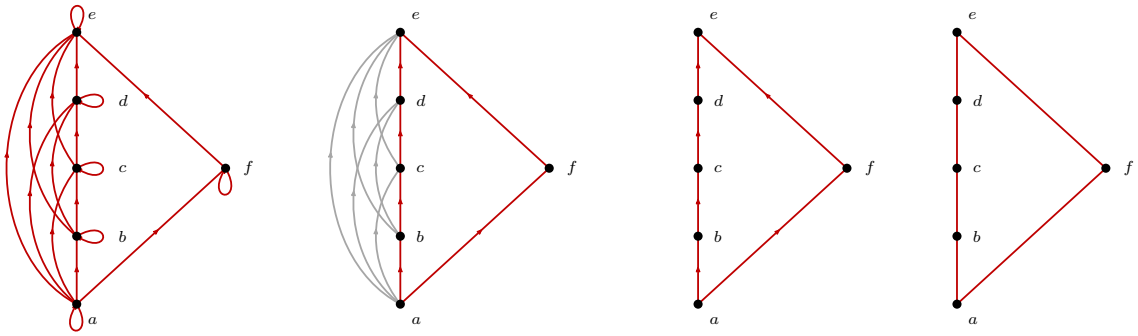


Figure 14: The four steps on a six-element partial order. First: the arrow diagram, already arranged so that every arrow points upward. It has 18 arrows. Second: the six loops are deleted, leaving 12. The six arrows that the transitive property implies are drawn in grey: each of them skips over at least one element of the column. Third: those are deleted, leaving six arrows, each from an element to one directly above it. Fourth: the arrowheads are deleted, since every line is understood to point up. What is left is the Hasse diagram.

Nothing is lost by the deleting. The removed arrows can all be put back, because the steps only take away what the three properties guarantee (hasse-diagrams[33]).

Worked: the Hasse diagram of a power set

Draw a Hasse diagram for the partial order relation $\subseteq$ on $\mathcal{P}(\{1, 2, 3\})$.

$\emptyset$ goes at the bottom, then $\{1\}$, $\{2\}$, $\{3\}$, then $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, and $\{1, 2, 3\}$ at the top, joined by twelve lines. The shape is a cube standing on one corner.

The arrow diagram of proper subset on the same eight sets has 19 arrows (2026-09-17-relations-reflexivity-symmetry-transitivity[34]). The relation $\subseteq$ has those 19 and a loop at each of the 8 sets, 27 arrows in all. The Hasse diagram keeps 12 of them: the ones that add a single element.

[33] courses/math1061/hasse-diagrams.pdf
[34] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf

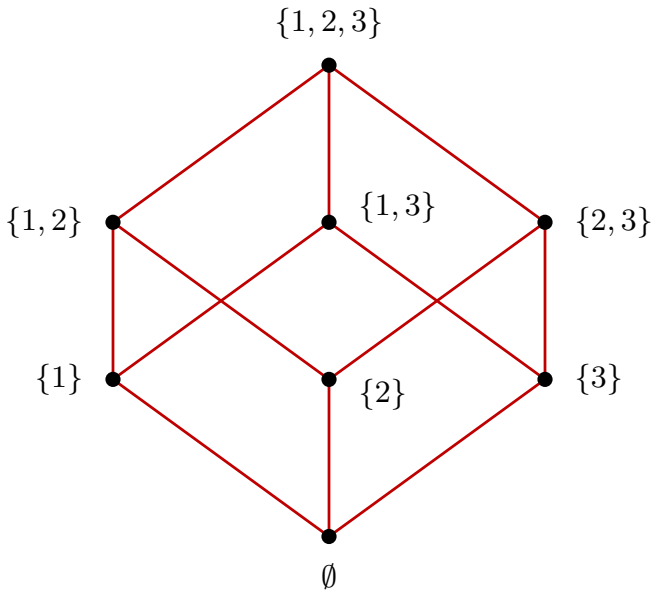


Figure 15: The Hasse diagram of $\subseteq$ on $\mathcal{P}(1,2,3)$. Each line joins a set to a set with exactly one more element. One set is a subset of another exactly when there is a path from the first up to the second, so $1 \subseteq 1,2,3$ by way of $1,2$ or $1,3$. Sets on the same level are never comparable. The twelve lines are the edges of a cube.

See also

- antisymmetric-relations[35] — the three equivalent definitions, and symmetric against antisymmetric
- partial-order-relations[36] — comparable elements, partial and total orders, and the proof template
- hasse-diagrams[37] — drawing one, and reading the relation back off it
- equivalence-classes-and-partitions[38] — classes and partitions, for the two questions at the start
- divisibility-and-factorisation[39] — the definition of "divides"
- 2026-09-21-equivalence-relations[40] — Lecture 24 · 2026-09-24-definitions-and-examples-of-groups[41] — Lecture 26
- practice-problems[42] — §32, with full worked solutions

Lecture 26 — Definitions and Examples of Groups

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], $\mathbb{Z}_n$ and arithmetic with equivalence classes in integers-modulo-n[43], reading a group off its table in cayley-tables[44], and S_n and S_3 in symmetric-group[45].

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:

- **How do addition and multiplication of equivalence classes work in $\mathbb{Z}_n$?** The next section.

[35] courses/math1061/antisymmetric-relations.pdf
[36] courses/math1061/partial-order-relations.pdf
[37] courses/math1061/hasse-diagrams.pdf
[38] courses/math1061/equivalence-classes-and-partitions.pdf
[39] courses/math1061/divisibility-and-factorisation.pdf
[40] courses/math1061/2026-09-21-equivalence-relations.pdf
[41] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[42] courses/math1061/practice-problems.pdf
[43] courses/math1061/integers-modulo-n.pdf
[44] courses/math1061/cayley-tables.pdf
[45] courses/math1061/symmetric-group.pdf

- **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[46]). $\mathbb{Z}_n$ 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.

[46] 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[47].

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, $x^{-1} = -x$

[47] 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[48].

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[49]).

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 $[2] \cdot [6] = [12] = [5]$.

[48] courses/math1061/groups.pdf
[49] 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[50], and composition is composition-of-functions[51].

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.

[50] courses/math1061/one-to-one-and-onto-functions.pdf
[51] courses/math1061/composition-of-functions.pdf

·	[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 16: 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 $f_1 \circ f_2 = f_2$.

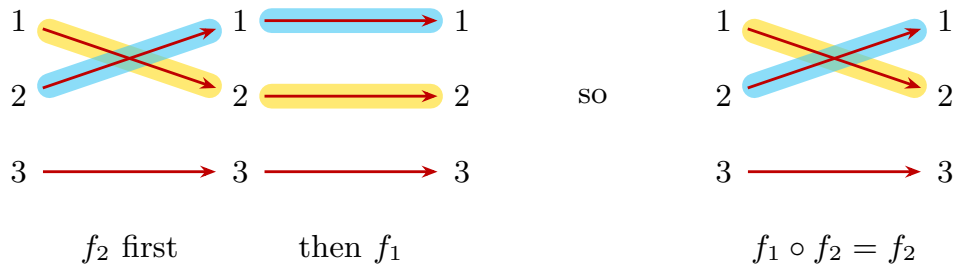


Figure 17: $f_1 \circ f_2$ in two steps. Follow each number through f_2 first and then through f_1. The yellow route takes 1 to 2 and then leaves it at 2, so $(f_1 \circ f_2)(1) = 2$. The cyan route takes 2 to 1 and leaves it there, so $(f_1 \circ f_2)(2) = 1$. Joining the start of each route directly 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

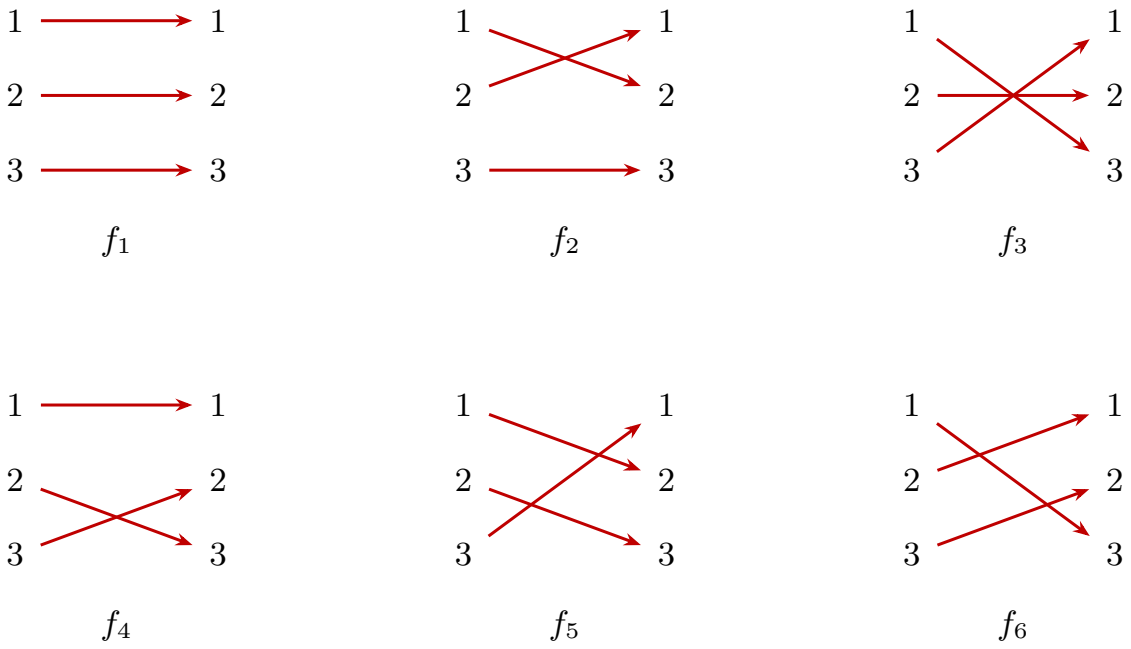


Figure 18: The six elements of S_3, every bijection from $1, 2, 3$ to itself. f_1 moves nothing. f_2, f_3 and f_4 each swap two numbers and leave the third alone: f_2 swaps 1 and 2, f_3 swaps 1 and 3, f_4 swaps 2 and 3. f_5 and f_6 move all three numbers round, in opposite directions.

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.

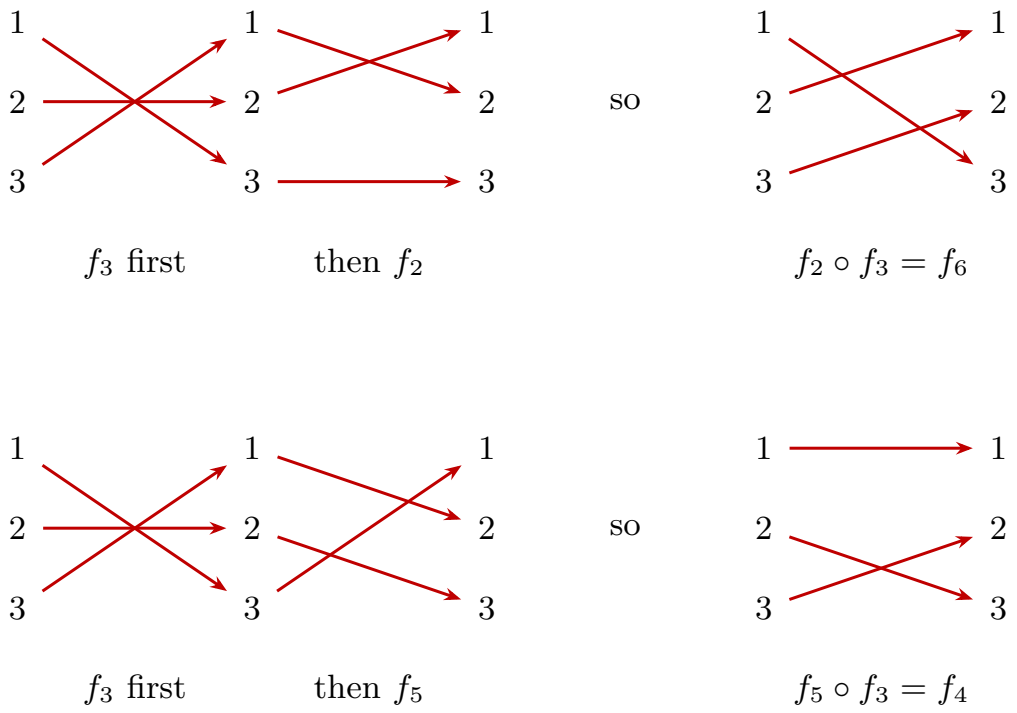


Figure 19: Two entries of the table, worked out. Top: $f_2 \circ f_3$. Do f_3 first, then f_2: 1 goes to 3 and stays, 2 stays and then goes to 1, 3 goes to 1 and then to 2. Overall $1 \to 3$, $2 \to 1$, $3 \to 2$, which is f_6. Bottom: $f_5 \circ f_3$. Do f_3 first, then f_5: 1 goes to 3 and then back 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 20: 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[52].

See also

- [groups] — the four properties, abelian groups, and the eight candidates checked one by one
- integers-modulo-n[53] — $\mathbb{Z}_n$ as a set of equivalence classes, and why any representative can be used
- cayley-tables[54] — reading identity, inverses and commutativity off a table, and why rows and columns have no repeats
- symmetric-group[55] — S_n, the six elements of S_3, and composing them
- composition-of-functions[56] · one-to-one-and-onto-functions[57] — the operation and the elements of S_n

[52] courses/math1061/cayley-tables.pdf
[53] courses/math1061/integers-modulo-n.pdf
[54] courses/math1061/cayley-tables.pdf
[55] courses/math1061/symmetric-group.pdf
[56] courses/math1061/composition-of-functions.pdf
[57] courses/math1061/one-to-one-and-onto-functions.pdf

- 2026-09-22-partial-order-relations[58] — Lecture 25 · 2026-10-06-elementary-properties-of-groups[59] — Lecture 27
- practice-problems[60] — §33, with full worked solutions

Reference material

Antisymmetric Relations

A relation is antisymmetric when no two *different* elements are related in both directions. It is the property that takes the place of symmetry in a partial order (partial-order-relations[61]). In spite of the name it is not the opposite of symmetric. The other three properties are in reflexive-symmetric-and-transitive-relations[62]. First met in 2026-09-22-partial-order-relations[63].

The definition

A relation R on a set S is **antisymmetric** if and only if

$$\forall a, b \in S,\ (a\ R\ b \text{ and } b\ R\ a) \to (a = b).$$

There are two **equivalent definitions**:

$$\forall a, b \in S,\ (a \neq b) \to \sim(a\ R\ b \text{ and } b\ R\ a).$$
$$\forall a, b \in S,\ (a\ R\ b \text{ and } a \neq b) \to \sim(b\ R\ a).$$

The first is the **easiest for proving** a relation antisymmetric, and the third is the most **intuitive**.

	In words
first	If a and b are related both ways, they are the same element.
second	Two different elements are not related both ways.

[58] courses/math1061/2026-09-22-partial-order-relations.pdf
[59] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[60] courses/math1061/practice-problems.pdf
[61] courses/math1061/partial-order-relations.pdf
[62] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[63] courses/math1061/2026-09-22-partial-order-relations.pdf

	In words
third	If a is related to a different element b, then b is not related back to a.

Why the three say the same thing

Write p for $a\ R\ b$, q for $b\ R\ a$ and r for $a = b$. The three definitions are the conditionals

$$(p \wedge q) \to r, \qquad \sim r \to \sim(p \wedge q), \qquad (p \wedge \sim r) \to \sim q.$$

The second is the contrapositive of the first (conditional-statements[64]). For the third, recall that a conditional is false in only one situation, a true hypothesis with a false conclusion. Work out that situation for each:

Conditional	False exactly when
$(p \wedge q) \to r$	p true, q true, r false
$\sim r \to \sim(p \wedge q)$	r false, p true, q true
$(p \wedge \sim r) \to \sim q$	p true, r false, q true

It is the same situation each time, so the three are logically equivalent. Each one forbids exactly one thing: $a\ R\ b$ **and** $b\ R\ a$ **with** $a \neq b$.

In the arrow diagram

Antisymmetric: no two different dots are joined by arrows both ways. Loops are not restricted. When $a = b$ the first definition reads ($a\ R\ a$ and $a\ R\ a$) $\to$ ($a = a$), which is true whether or not there is a loop at a.

Between two different elements there are three possibilities, and symmetry and antisymmetry each rule out a different one.

Antisymmetric is not "not symmetric"

Antisymmetric $\neq$ not symmetric. The two properties are independent, and all four combinations occur. The diagrams are the four of 2026-09-22-partial-order-relations[65].

[64] courses/math1061/conditional-statements.pdf
[65] courses/math1061/2026-09-22-partial-order-relations.pdf

between two different elements		symmetric	antisymmetric
	no arrow	✓ allowed	✓ allowed
	one arrow	× no return	✓ allowed
	arrows both ways	✓ allowed	× but $a \neq b$
	a loop	✓ allowed	✓ allowed

Figure 21: What symmetry and antisymmetry allow between two different elements. With no arrow, both are satisfied. A single arrow has no return, which breaks symmetry and is fine for antisymmetry. Arrows both ways are what symmetry asks for, and they break antisymmetry. So a symmetric relation has no single arrows, and an antisymmetric relation has no two-way pairs. A loop joins an element to itself and breaks neither.

	antisymmetric	**not antisymmetric**
symmetric	Diagram 2. Only loops. Also: $=$ on any set.	Diagram 3. Two-way pairs, no single arrows. Also: same parity on $\mathbb{Z}$.
not symmetric	Diagram 4. Single arrows, no two-way pairs. Also: $\leq$ on $\mathbb{R}$, $\subseteq$, divides on $\mathbb{Z}^+$.	Diagram 1. A single arrow and a two-way pair.

The definitions make the difference exact:

- **not symmetric** says *there is* an arrow with no return;
- **antisymmetric** says *no* arrow between different elements has a return.

A relation that is not symmetric can still have some two-way pairs, as Diagram 1 does, and then it is not antisymmetric either.

Both at once. If R is symmetric and antisymmetric, every arrow is a loop. Suppose $a \; R \; b$. Symmetry gives $b \; R \; a$, and then antisymmetry gives $a = b$. So the only relations with both properties are those in which no element is related to anything but itself, like Diagram 2.

Proving and disproving

Antisymmetry is a "for all", so it is proved with arbitrary elements and disproved with one witness.

	How
To prove it	Let $a, b \in S$ and suppose $a \; R \; b$ **and** $b \; R \; a$. Unfold both. Show $a = b$.
To disprove it	Find two **different** elements a, b with $a \; R \; b$ and $b \; R \; a$.

In the proof, write the goal down before starting: *(Goal: show $a = b$).* Both hypotheses will be needed.

Worked: divides on $\mathbb{Z}^+$

Worked in full in 2026-09-22-partial-order-relations[66]. Let $a, b \in \mathbb{Z}^+$ and suppose $a \mid b$ and $b \mid a$. *(Goal: show $a = b$.)* Then $b = ak$ and $a = b\ell$ for some $k, \ell \in \mathbb{Z}$. Substituting,

$$b = ak = (b\ell)k = b(\ell k),$$

[66] courses/math1061/2026-09-22-partial-order-relations.pdf

and since $b \neq 0$, $\ell k = 1$. Now $a, b > 0$ forces $k > 0$ and $\ell > 0$, and the only positive integers with product 1 are $\ell = k = 1$. So $a = b$.

The last step uses that the set is $\mathbb{Z}^+$. See Examples for what goes wrong on $\mathbb{Z}$.

Worked: a disproof

From practice-problems[67], Q2. On binary strings of length 6, let $s \rho t$ if and only if weight$(s) \leq$ weight(t), where the weight is the number of ones. Take $s = 100000$ and $t = 010000$. Both have weight 1, so $s \rho t$ and $t \rho s$, but $s \neq t$. So ρ is not antisymmetric.

Two different things with the same weight are related both ways. Any relation that compares elements through a number they can share fails in the same way.

The third form in a proof

The first definition is the easiest to prove from, but the third works too. The solution to practice-problems[68], Q1 uses it: *suppose* $x \rho y$ *where* $x \neq y$*; we must show that then* $y \not\rho x$. Either is acceptable. State which you are using.

Examples

The standard examples, with reasons:

Relation	on	Antisymmetric because
$\leq$	$\mathbb{R}$	$(x \leq y$ and $y \leq x) \to x = y$
$\geq$	$\mathbb{R}$	the same, reversed
$<$, $>$	$\mathbb{R}$	$x < y$ and $y < x$ never hold together
divides	$\mathbb{Z}^+$	proved above
$\subseteq$	any set S of sets	$(X \subseteq Y$ and $Y \subseteq X) \to X = Y$

$<$ is antisymmetric vacuously. For no x, y are $x < y$ and $y < x$ both true. The hypothesis of the first definition is therefore always false, and a conditional with a false hypothesis is true (conditional-statements[69]). In the diagram of $<$ there are no two-way pairs, and no loops either.

[67] courses/math1061/practice-problems.pdf
[68] courses/math1061/practice-problems.pdf
[69] courses/math1061/conditional-statements.pdf

$\subseteq$ is the double-containment rule. Showing $X \subseteq Y$ and $Y \subseteq X$ to conclude $X = Y$ is how set equality is proved (sets-and-set-notation[70]). Antisymmetry of $\subseteq$ is that rule under another name.

Divides is not antisymmetric on $\mathbb{Z}$. $2 \mid -2$, since $-2 = 2 \cdot (-1)$, and $-2 \mid 2$, since $2 = (-2)(-1)$, but $2 \neq -2$. This is why the statement is about $\mathbb{Z}^+$. A relation is always a relation on a particular set, and the same rule on a bigger set can lose a property.

Not antisymmetric: any relation with two different elements related both ways. That includes congruence mod n for $n \geq 1$, same parity, and every equivalence relation that has a class with more than one element.

Common mistakes

- **Reading "antisymmetric" as "not symmetric".** See the four combinations above.
- **Thinking a loop breaks antisymmetry.** It does not. The property is about pairs of *different* elements.
- **Proving it from an example.** "$2 \mid 4$ but $4 \nmid 2$" shows one pair behaves. Antisymmetry is about all pairs.
- **Using only one hypothesis.** A proof that starts "suppose $a \; R \; b$" and never uses $b \; R \; a$ cannot reach $a = b$.
- **Disproving with $a = b$.** A witness needs two different elements. $a \; R \; a$ on its own shows nothing.

See also

- partial-order-relations[71] — reflexive, antisymmetric and transitive together
- reflexive-symmetric-and-transitive-relations[72] — the other three properties, and how to prove and disprove them
- conditional-statements[73] — the contrapositive, and vacuous truth
- divisibility-and-factorisation[74] — the definition of divides
- 2026-09-22-partial-order-relations[75] — Lecture 25
- practice-problems[76] — §32, with full worked solutions

[70] courses/math1061/sets-and-set-notation.pdf
[71] courses/math1061/partial-order-relations.pdf
[72] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[73] courses/math1061/conditional-statements.pdf
[74] courses/math1061/divisibility-and-factorisation.pdf
[75] courses/math1061/2026-09-22-partial-order-relations.pdf
[76] courses/math1061/practice-problems.pdf

Cayley Tables

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]. The tables for $\mathbb{Z}_7 - \{[0]\}$ and for S_3 are built in 2026-09-24-definitions-and-examples-of-groups[77]. With the right ordering of the headings, a subgroup shows up as a block of the table (below, and subgroups-and-cyclic-groups[78]).

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[79]). The entry in row f_3, column f_2 is a different element, f_5.

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[80]).

[77] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[78] courses/math1061/subgroups-and-cyclic-groups.pdf
[79] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[80] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

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[81], Q4.

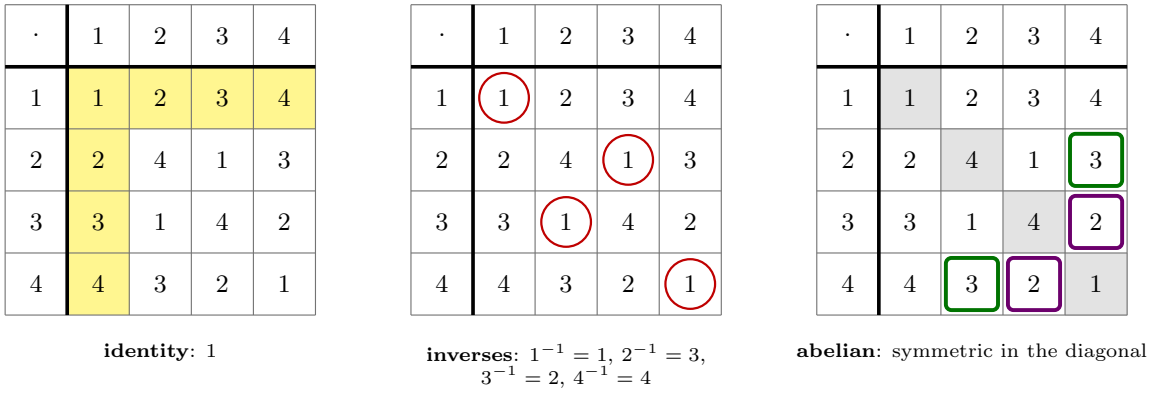


Figure 22: Three readings of one table, $\mathbb{Z}_5 - [0]$ under multiplication, written without brackets. Left: the row and the column of 1, in yellow, repeat the headings, so 1 is the identity. Middle: the identity appears once in every row. The ring in row 2 is in column 3, so $2^{-1} = 3$; the 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 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.

Rows. By contradiction (2026-09-24-definitions-and-examples-of-groups[82]). 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

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

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.

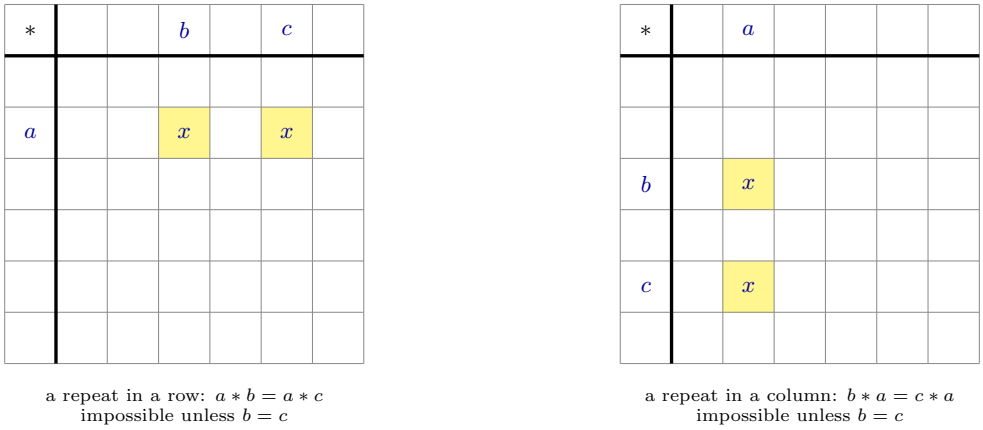


Figure 23: What the two results forbid. Left: the same element x twice in the row of a, in the columns of two different elements b and c. That would mean $a * b = a * c$, and applying a^{-1} on the left gives $b = c$. Right, the column version: the same x twice in the column of a, which would mean $b * a = c * a$, and applying a^{-1} on the right gives $b = c$. Neither picture can occur in the table of a group.

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.

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 $\{1, \dots, 8\}$ 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[83], 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.

Subgroups in a table

A subgroup is a subset that is a group under the same operation (subgroups-and-cyclic-groups[84]). 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[85]. The same works in a non-abelian group. In S_3, list f_1, f_5, f_6 first:

[83] courses/math1061/practice-problems.pdf
[84] courses/math1061/subgroups-and-cyclic-groups.pdf
[85] courses/math1061/2026-10-06-elementary-properties-of-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 24: 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.

$\{f_1, f_5, f_6\}$ 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[86]).

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[87]
$(S_3, \circ)$	6	**no**	2026-09-24-definitions-and-examples-of-groups[88]
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	4	yes	practice-problems[89], Q4; above
$(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$	4	yes	the same practice set, Q5
$(\mathbb{Z}_3, +)$	3	yes	integers-modulo-n[90]
$(\mathbb{Z}_6, +)$, even classes first	6	yes	2026-10-06-elementary-properties-of-groups[91]
$(S_3, \circ)$, 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.

[86] courses/math1061/symmetric-group.pdf
[87] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[88] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[89] courses/math1061/practice-problems.pdf
[90] courses/math1061/integers-modulo-n.pdf
[91] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

- **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] — the four properties the table is checked against, and cancellation as solving $a * x = b$
- integers-modulo-n[92] — the groups $\mathbb{Z}_n$ and $\mathbb{Z}_n - \{[0]\}$ behind the first tables
- symmetric-group[93] — S_3, whose table is not symmetric
- subgroups-and-cyclic-groups[94] — subgroups and cyclic subgroups, the blocks found above
- proof-techniques[95] — proof by contradiction, the method of the rows result
- 2026-09-24-definitions-and-examples-of-groups[96] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[97] — Lecture 27 · 2026-10-08-definitions-and-examples-of-fields[98] — Lecture 28, where the table of $\mathbb{Z}_4 - \{[0]\}$ fails closure
- practice-problems[99] — §33, with full worked solutions

Composition of Functions

Chaining two functions into one, and which properties survive the chaining — in both directions. First met in 2026-09-08-composition-of-functions[100]; the properties are defined in one-to-one-and-onto-functions[101] and inverse-functions[102].

Definition

> Let $f : X \to Y$ and $g : Y \to Z$ be functions. The **composition** of f and g is the function $g \circ f : X \to Z$ defined by
>
> $$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in X.$$

[92] courses/math1061/integers-modulo-n.pdf
[93] courses/math1061/symmetric-group.pdf
[94] courses/math1061/subgroups-and-cyclic-groups.pdf
[95] courses/math1061/proof-techniques.pdf
[96] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[97] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[98] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[99] courses/math1061/practice-problems.pdf
[100] courses/math1061/2026-09-08-composition-of-functions.pdf
[101] courses/math1061/one-to-one-and-onto-functions.pdf
[102] courses/math1061/inverse-functions.pdf

Three things to read off the definition:

- **Right to left.** $g \circ f$ applies f *first*, then g. The order of the symbols matches the formula $g(f(x))$, not the order of events.
- **The domain of $g \circ f$ is the domain of f; the co-domain is the co-domain of g.** The middle set Y vanishes from the type.
- **It is defined only when f's co-domain is g's domain.** $g \circ f$ makes sense because f lands in Y and g eats Y. The other composite, $f \circ g$, would need g's outputs (in Z) to be inputs to f (from X), so it exists only if $Z = X$.

The composition itself is drawn in 2026-09-08-composition-of-functions[103]: three ellipses, $x \mapsto f(x) \mapsto g(f(x))$, with the long arrow $g \circ f$ beneath.

Composition is not commutative. Even when both orders exist ($X = Y = Z$), $g \circ f$ and $f \circ g$ are generally different functions: with $f(x) = x+1$ and $g(x) = 2x$ on $\mathbb{R}$, $(g \circ f)(x) = 2x+2$ but $(f \circ g)(x) = 2x + 1$.

Inverses and composition

For a bijection $f : X \to Y$ with inverse $f^{-1} : Y \to X$ (inverse-functions[104]), both composites exist and both do nothing:

$$(f^{-1} \circ f)(x) = x \text{ for all } x \in X, \qquad (f \circ f^{-1})(y) = y \text{ for all } y \in Y.$$

This is the **sense check** on a computed inverse: for $f((x, y)) = (y + 1, 2x)$ and the claimed $f^{-1}((x, y)) = (\frac{y}{2}, x - 1)$,

$$f(f^{-1}((x, y))) = f((\tfrac{y}{2}, x - 1)) = (x, y). \checkmark$$

Which properties compose

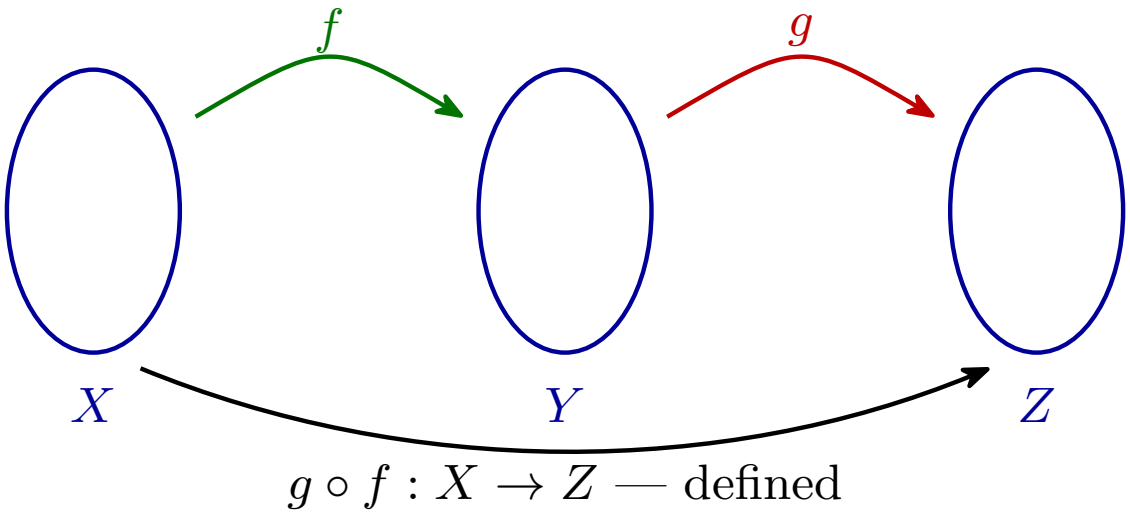
Two facts:

> If f and g are both **onto**, then $g \circ f$ is onto. If f and g are both **one-to-one**, then $g \circ f$ is one-to-one.

So both bijective gives $g \circ f$ bijective. The proofs are short:

- *Onto.* Let $z \in Z$. Since g is onto, $\exists\, y \in Y$ with $g(y) = z$. Since f is onto, $\exists\, x \in X$ with $f(x) = y$. Then $g(f(x)) = z$. $\square$
- *One-to-one.* Suppose $g(f(x_1)) = g(f(x_2))$. Since g is one-to-one, $f(x_1) = f(x_2)$. Since f is one-to-one, $x_1 = x_2$. $\square$

[103] courses/math1061/2026-09-08-composition-of-functions.pdf
[104] courses/math1061/inverse-functions.pdf



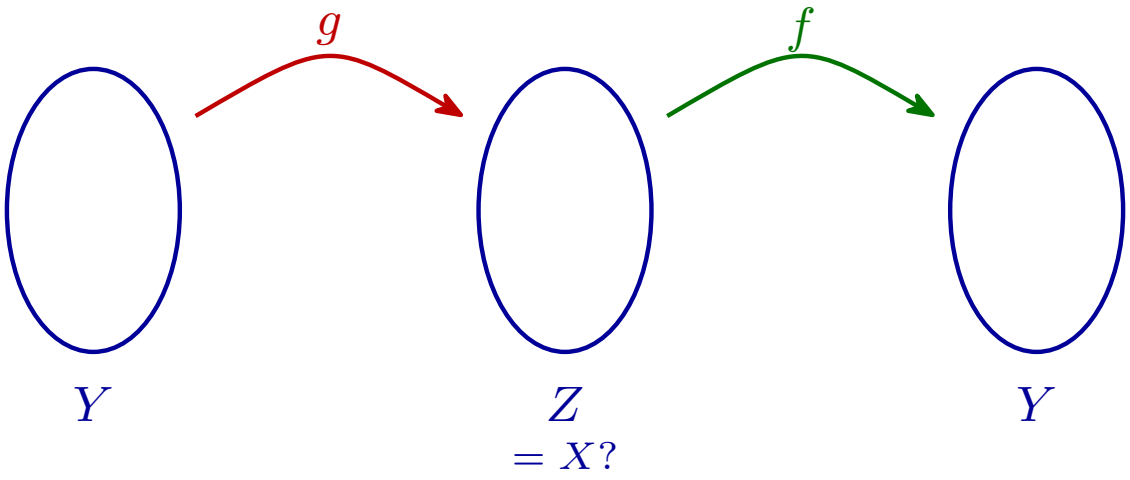


Figure 25: Why $g \circ f$ exists and $f \circ g$ usually does not. Top: f then g chains because f lands exactly where g starts. Bottom: g then f would need g's outputs, in Z, to be acceptable inputs to f, which come from X — so it is defined only if $Z = X$.

Which properties come back

The converse asks which ingredient must have a property when the **composite** has it. The answer is asymmetric:

If $g \circ f$ is …	then f must be …	then g must be …
onto	*not necessarily*	**onto**
one-to-one	**one-to-one**	*not necessarily*

The property comes back to the function on its own side. Onto is about covering Z, and g is the function that lands in Z. One-to-one is about not merging elements of X, and f is the function that leaves X. The other ingredient can misbehave in the middle set Y without the composite noticing, as long as the misbehaviour is never exercised.

The two theorems, by contraposition

If $g \circ f$ is onto, then g is onto.

Proof. We prove the contrapositive: if g is not onto then $g \circ f$ is not onto. Suppose g is not onto. Then $\exists\, z \in Z$ not in the range of g. Then no $x \in X$ has $g(f(x)) = z$ — for if one did, $y = f(x)$ would have $g(y) = z$, a contradiction. So z is not in the range of $g \circ f$, and $g \circ f$ is not onto. □

If $g \circ f$ is one-to-one, then f is one-to-one.

Proof. We prove the contrapositive: if f is not one-to-one then $g \circ f$ is not one-to-one. Suppose f is not one-to-one. Then $\exists\, x_1 \neq x_2 \in X$ with $f(x_1) = f(x_2)$. Hence $g(f(x_1)) = g(f(x_2))$, i.e. $(g \circ f)(x_1) = (g \circ f)(x_2)$ with $x_1 \neq x_2$, so $g \circ f$ is not one-to-one. □

Both go by contraposition (proof-techniques[105]) for the same reason: *not onto* and *not one-to-one* are **existential** and hand you a concrete witness — a missed z, a colliding pair — to push through the composite. The positive forms are universal and give nothing to hold onto. Anything the composite reaches, g reaches; anything f merges, the composite merges.

[105] courses/math1061/proof-techniques.pdf

The two counterexamples, to order

> $g \circ f$ **onto does not force** f **onto.** $X = \{a, b\}$, $Y = \{0, 1, 2\}$, $Z = \{v, w\}$; $f = \{(a, 0), (b, 1)\}$, $g = \{(0, v), (1, w), (2, w)\}$. Then f misses 2, but $g \circ f = \{(a, v), (b, w)\}$ is onto.

> $g \circ f$ **one-to-one does not force** g **one-to-one.** $X = \{a, b\}$, $Y = \{1, 2, 3\}$, $Z = \{u, v\}$; $f = \{(a, 1), (b, 2)\}$, $g = \{(1, u), (2, v), (3, v)\}$. Then $g(2) = g(3)$, but $g \circ f = \{(a, u), (b, v)\}$ is one-to-one.

Both are drawn in 2026-09-08-composition-of-functions[106], as (1) and (4) there, and both are built by the same recipe, which is the transferable skill:

1. **Make Y one element bigger than it needs to be.** That spare element is where the defect will live.
2. **Give the defect to the function on the wrong side.** For (1) f must *miss* the spare element; for (4) g must *merge* the spare element with another.
3. **Make sure the composite never touches it.** In (1), g sends the missed element somewhere already covered, so the gap is invisible from Z. In (4), f never lands on the merged element, so the collision is never fed.
4. **Use small sets.** Two-element X and Z with a three-element Y, as above, is enough; even smaller works. A counterexample is a witness; it does not need to be interesting.

The mirror symmetry is exact: (1) is *gap in f, hidden by a merge in g*; (4) is *merge in g, hidden by a gap in f*.

See also

- one-to-one-and-onto-functions[107] — the properties and their proof templates
- inverse-functions[108] — $f \circ f^{-1}$ as the identity
- symmetric-group[109] — composition as the operation of a group, on the bijections of $\{1, \ldots, n\}$
- groups[110] — the functions $ax+b$ with $a \neq 0$, a second non-abelian group under composition
- proof-techniques[111] — contraposition and counterexample
- 2026-09-08-composition-of-functions[112] — Lecture 20 · 2026-09-07-functions-one-to-one-onto-inverse[113] — Lecture 19

[106] courses/math1061/2026-09-08-composition-of-functions.pdf
[107] courses/math1061/one-to-one-and-onto-functions.pdf
[108] courses/math1061/inverse-functions.pdf
[109] courses/math1061/symmetric-group.pdf
[110] courses/math1061/groups.pdf
[111] courses/math1061/proof-techniques.pdf
[112] courses/math1061/2026-09-08-composition-of-functions.pdf
[113] courses/math1061/2026-09-07-functions-one-to-one-onto-inverse.pdf

- practice-problems[114] — §26

Countable and Uncountable Sets

Which infinite sets are the same size as $\mathbb{Z}^+$, and which are strictly bigger. A set is **countable** when its elements can be listed, and **uncountable** when no list can contain them all. Sizes are compared with bijections and injections, as set out in cardinality[115]. The lectures are 2026-09-14-cardinalities[116] (the listings) and 2026-09-15-countable-and-uncountable-sets[117] (the definitions and the uncountable sets).

The definitions

A set X is **finite** if and only if $X = \emptyset$ or $|X| = |\{1, 2, \dots, n\}|$ for some $n \in \mathbb{Z}^+$.

A set is **infinite** if and only if it is not finite.

A set X is **countable** if and only if it is finite or $|X| = |\mathbb{Z}^+|$.

A set X is **uncountable** if and only if it is not countable.

A set X is **countably infinite** if and only if it is countable and infinite.

Every set falls in exactly one of three classes, and "countable" and "infinite" each cover two of them:

	finite	**countably infinite**	**uncountable**
countable?	yes	yes	no
infinite?	no	yes	yes
$\lvert X\rvert$	0 or n	$\lvert\mathbb{Z}^+\rvert$	$> \lvert\mathbb{Z}^+\rvert$
examples	$\emptyset$, $\{1, \dots, n\}$, $\{0, 1\}$	$\mathbb{Z}^+$, $2\mathbb{Z}$, $\mathbb{Z}$, $\mathbb{Q}^+$, $\mathbb{Q}$, $\mathbb{Z} \times \mathbb{Z}$	$(0, 1)$, $\mathbb{R}$, $\mathcal{P}(\mathbb{Z}^+)$

The trap is that **countable includes finite**. "Countable" is not a word for a kind of infinity; "countably infinite" is.

[114] courses/math1061/practice-problems.pdf
[115] courses/math1061/cardinality.pdf
[116] courses/math1061/2026-09-14-cardinalities.pdf
[117] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf

Listing a set

> X is countably infinite if and only if the elements of X can be written as an infinite list, $X = \{x_1, x_2, x_3, \dots\}$, where the x_i are all distinct.

A list *is* a bijection $f : \mathbb{Z}^+ \to X$, $f(i) = x_i$. "All distinct" is one-to-one, and "every element of X is somewhere in the list" is onto. To show a set is countably infinite it is enough to describe a list and convince yourself of those two things.

The listings that matter:

Set	List	Where
$2\mathbb{Z}^+$	$2, 4, 6, 8, \dots$	2026-09-14-cardinalities[118]
$\mathbb{Z}$	$0, 1, -1, 2, -2, 3, -3, \dots$	Figure 26; as a formula in cardinality[119]
$\mathbb{Q}^+$	along the anti-diagonals of the $\frac{a}{b}$ grid, skipping repeats	2026-09-14-cardinalities[120]
$\mathbb{Z} \times \mathbb{Z}$	out along a square spiral from $(0, 0)$	2026-09-14-cardinalities[121]
$\mathbb{Q}$	along the same spiral, counting only lowest-terms pairs (a, b), with the sign kept in one fixed place (here $b \geq 1$)	2026-09-14-cardinalities[122]

They are all built the same way. **Break the set into finite batches that together cover it, and list the batches one after another.** Because each batch is finite, every element comes up after finitely many steps. The batches are $\{n, -n\}$ for $\mathbb{Z}$, the anti-diagonals $a + b = s$ for $\mathbb{Q}^+$, and the square rings for $\mathbb{Z} \times \mathbb{Z}$.

Subsets of countable sets

> **Theorem:** Any subset of a countable set is countable.
>
> **Corollary:** Any set with an uncountable subset is uncountable.

The corollary is the contrapositive of the theorem. For the theorem, take a list of the countable set, keep the members of the subset in the order they come up, and cross out the rest. What is left is a list of the subset, finite if only finitely many survive. The key special case:

[118] courses/math1061/2026-09-14-cardinalities.pdf
[119] courses/math1061/cardinality.pdf
[120] courses/math1061/2026-09-14-cardinalities.pdf
[121] courses/math1061/2026-09-14-cardinalities.pdf
[122] courses/math1061/2026-09-14-cardinalities.pdf

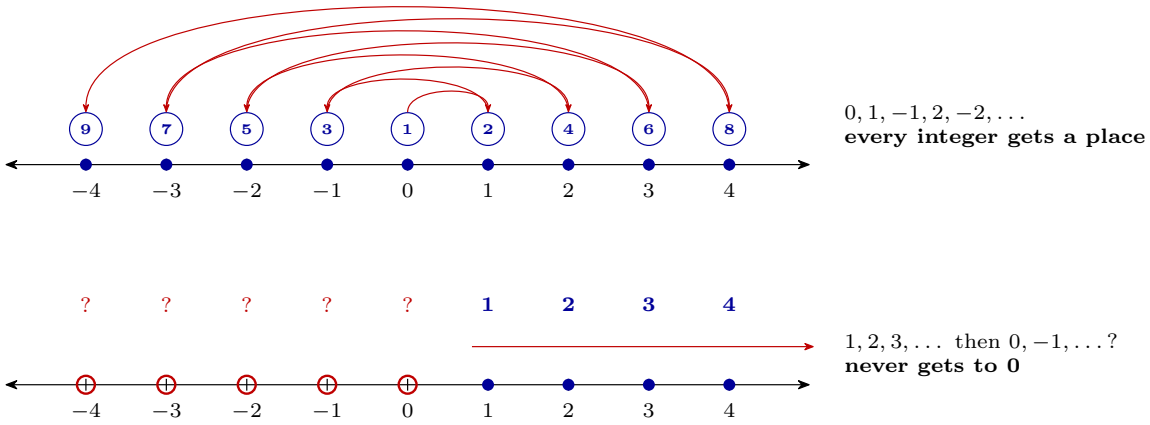


Figure 26: Two attempts to list $\mathbb{Z}$; the number above each integer is its place in the list. Top: alternating out from 0 — $0, 1, -1, 2, -2, \ldots$ — reaches every integer after finitely many steps ($-n$ is in place $2n+1$), so it is a list of all of $\mathbb{Z}$. Bottom: all the positive integers first never finishes them, so 0 and the negatives never get a place, and it is not a list of $\mathbb{Z}$ at all. A listing must reach every element after finitely many steps; going out in finite batches, here the pairs $n, -n$, is how to guarantee it.

Every infinite subset of $\mathbb{Z}^+$ has the same cardinality as $\mathbb{Z}^+$.

Proof. Let $A \subseteq \mathbb{Z}^+$ be infinite. Let a_1 be the least element of A, a_2 the least element of $A - \{a_1\}$, a_3 the least element of $A - \{a_1, a_2\}$, and so on. Each step is allowed by the well-ordering principle[123]: what is left is a set of positive integers, and it is non-empty because A is infinite. Define $f : \mathbb{Z}^+ \to A$ by $f(i) = a_i$.

- f is one-to-one, because $a_1 < a_2 < a_3 < \cdots$, so different positions hold different numbers.
- f is onto, because an element $a \in A$ has fewer than a elements of A below it, all positive integers less than a. So a is the least element left after at most $a - 1$ steps, and is picked as some a_j.

So $|\mathbb{Z}^+| = |A|$. □

$A \subseteq \mathbb{Z}^+$ is used twice: in the well-ordering step, which needs a least element at every stage, and in the onto step, "fewer than a elements below it". The same construction on $\mathbb{Q}^+$ itself breaks at the first of these, because there is no least positive rational, and that is why $\mathbb{Q}^+$ needed the grid.

[123] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

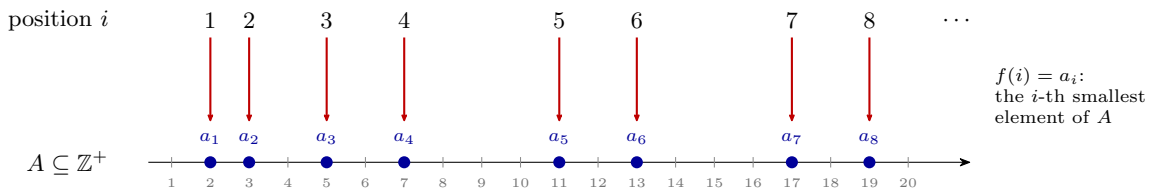


Figure 27: An infinite subset of $\mathbb{Z}^+$, the primes, listed by always taking the least element not yet used. The well-ordering principle guarantees a least element at every step, and the list is increasing, so no prime is used twice. No prime is skipped either: a prime p has only finitely many primes below it, so it is reached after finitely many steps — 13 has five primes below it and is sixth. So $i \mapsto a_i$ is a bijection from $\mathbb{Z}^+$ to the primes, and the primes, a sparse and irregular subset, are exactly as numerous as the positive integers.

$\mathbb{R}$ is uncountable

It is enough to show that the interval $(0, 1)$ is uncountable, because $(0, 1) \subseteq \mathbb{R}$ and the corollary does the rest.

Theorem. $(0, 1)$ is uncountable.

Proof (by contradiction). Suppose $(0, 1)$ is countable. It is infinite, so its elements can be written in a list $r_1, r_2, r_3, \ldots$. Write each as a decimal,

$$r_n = 0.\, d_{n1}\, d_{n2}\, d_{n3}\, \ldots$$

Define a number $d = 0.\, e_1\, e_2\, e_3\, \ldots$ digit by digit, from the **diagonal** digits $d_{11}, d_{22}, d_{33}, \ldots$:

$$e_n = \begin{cases} 1 & \text{if } d_{nn} \neq 1, \\ 2 & \text{if } d_{nn} = 1. \end{cases}$$

Then $d \in (0, 1)$. For every n, d differs from r_n in the n-th decimal place, so $d \neq r_n$. So d is not in the list, a contradiction. Hence $(0, 1)$ is uncountable, and so is $\mathbb{R}$. $\square$

This is **Cantor's diagonal argument**. It is worked on a concrete table in 2026-09-15-countable-and-uncountable-sets[124]. Three points in it are easy to get wrong:

- **It defeats every list, not one list.** The proof never uses anything about the particular list. Whatever list is proposed, the diagonal manufactures a number it misses. That is what "no bijection from $\mathbb{Z}^+$ exists" requires.

[124] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf

- **Why the digits 1 and 2.** Some numbers have two decimal expansions: $0.1999\ldots = 0.2000\ldots$. If d could end in all 0s or all 9s, "differs in a digit" might not mean "is a different number". A decimal made of 1s and 2s has only the one expansion, so it really is different from every r_n.
- **The same argument on $\mathbb{Q}$ fails.** The diagonal of a list of rationals produces a real number, and nothing forces it to be rational. So there is no contradiction, and indeed $\mathbb{Q}$ is countable.

Not only is $\mathbb{R}$ bigger than $\mathbb{Z}^+$, it is no bigger than the interval inside it: $|(0,1)| = |\mathbb{R}|$.

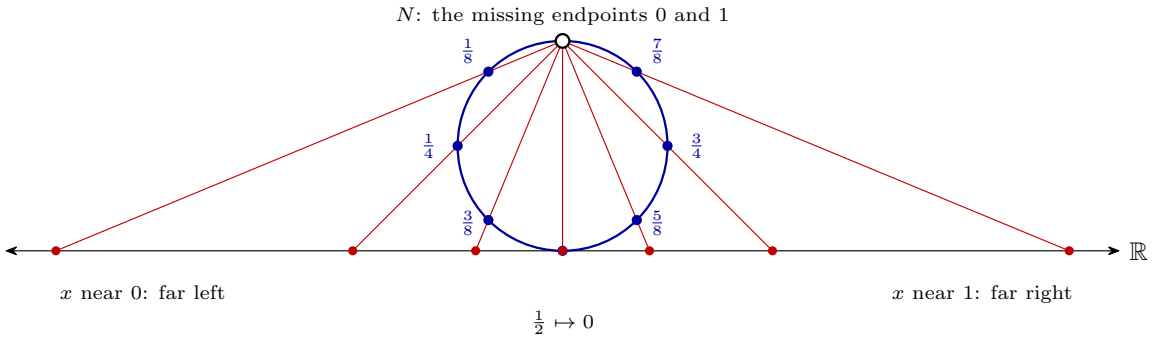


Figure 28: Why the open interval $(0,1)$ has as many points as the whole line. Bend $(0,1)$ into a circle resting on the line, so that its two missing endpoints would meet at the top point N, which is left out. A ray from N through any other point of the circle meets the line exactly once, and every point of the line is hit by exactly one such ray. Points near the top land far out, the bottom point lands at 0, and nothing is left over on either side — a bijection $(0,1) \to \mathbb{R}$.

The irrational numbers are uncountable as well. If they were countable, $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} - \mathbb{Q})$ would be a union of two countable sets and so countable (practice-problems[125], question 3).

The hierarchy

$$|\emptyset| < |\{1, 2, \ldots, n\}| < |\mathbb{Z}^+| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}| < |\mathcal{P}(\mathbb{R})|$$

Each strict step has a reason:

- $|\emptyset| < |\{1, \ldots, n\}|$**.** There is an injection from $\emptyset$ (the empty function), but no function at all from a non-empty set to $\emptyset$, so no bijection.
- $|\{1, \ldots, n\}| < |\mathbb{Z}^+|$**.** $\{1, \ldots, n\}$ sits inside $\mathbb{Z}^+$, but no bijection exists, since $\mathbb{Z}^+$ is not finite.
- $|\mathbb{Z}^+| < |\mathbb{R}|$**.** $\mathbb{Z}^+ \subseteq \mathbb{R}$ gives $\leq$, and the diagonal argument rules out $=$.

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

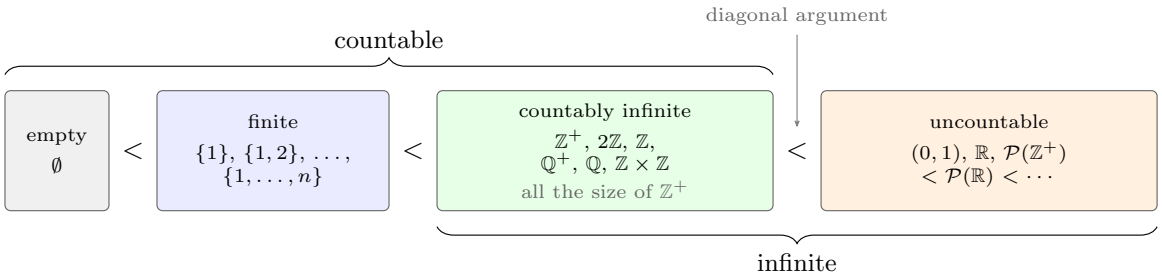


Figure 29: The sizes of sets met in the course, smallest on the left. Countable covers the first three blocks, empty, finite and countably infinite; infinite covers the last two. Within a block the sets have equal size wherever the chain above writes $=$: every countably infinite set is the size of $\mathbb{Z}^+$. Crossing a boundary is a strict step up, and the step from countably infinite to uncountable is the diagonal argument. The last block is not all one size: $\mathcal{P}(\mathbb{R})$ is strictly bigger than $\mathbb{R}$.

- **$|\mathbb{R}| < |\mathcal{P}(\mathbb{R})|$.** Stated without proof. *Beyond the course:* Cantor's theorem says $|A| < |\mathcal{P}(A)|$ for every set A, by a diagonal argument on subsets. So the chain never stops: $\mathcal{P}(\mathcal{P}(\mathbb{R}))$ is bigger again, and there is no largest size.

How to show a set is countable, or uncountable

Countable — any one of:

1. It is finite.
2. Write down a list, in finite batches, and check that every element appears exactly once.
3. Give a bijection with a set already known to be countable, such as $\mathbb{Z}^+$, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{Z}\times\mathbb{Z}$.
4. Give an **injection into** a countable set. The image is a subset of a countable set, so it is countable, and the injection is a bijection onto its image, so the set itself is countable too. With an injection the other way as well, Schröder–Bernstein gives the exact cardinality, as in the proof that $\mathbb{Z}^+\times\mathbb{Z}^+$ is countable using $(a,b)\mapsto 3^a5^b$ (2026-09-15-countable-and-uncountable-sets[126]).

Uncountable — any one of:

1. It contains an uncountable subset, such as an interval of $\mathbb{R}$.
2. There is an **injection from** a known uncountable set into it, for example from $(0,1)$.
3. A diagonal argument: assume a list, and build an element the list misses.

[126] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf

Whatever the direction, the argument has to be a proof. Not being able to think of a list does not show that none exists.

What is assessed. The course practice set marks its whole countable-and-uncountable section (§28) "not assessed in MATH1061", while Lecture 22 marks only the proof that $\mathbb{R}$ is uncountable and the countability of $\mathbb{Z}^+ \times \mathbb{Z}^+$ as not assessed. The two disagree, so check with the course.

See also

- cardinality[127] — bijections, the $|X| = |Y|$ template, $\leq$ by injection, Schröder–Bernstein
- strong-induction-and-the-well-ordering-principle[128] — the principle that lists an infinite subset of $\mathbb{Z}^+$
- proof-techniques[129] — proof by contradiction, the shape of the diagonal argument
- rational-and-irrational-numbers[130] — $\mathbb{Q}$ and $\overline{\mathbb{Q}}$, on either side of the countable line
- 2026-09-14-cardinalities[131] — Lecture 21 · 2026-09-15-countable-and-uncountable-sets[132] — Lecture 22
- practice-problems[133] — §28, with full worked solutions and the computability application

Divisibility & Unique Factorisation

Definition

$$d \mid n \iff d \neq 0 \text{ and } n = dk \text{ for some integer } k$$

Both n and d must be integers, and $d \neq 0$ — this side condition is part of the definition, not an afterthought. Equivalently, $d \mid n \iff \frac{n}{d} \in \mathbb{Z}$.

All of these say the same thing:

- d divides n
- d is a divisor of n
- d is a factor of n
- n is a multiple of d

[127] courses/math1061/cardinality.pdf
[128] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[129] courses/math1061/proof-techniques.pdf
[130] courses/math1061/rational-and-irrational-numbers.pdf
[131] courses/math1061/2026-09-14-cardinalities.pdf
[132] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf
[133] courses/math1061/practice-problems.pdf

$d \nmid n$ means d does not divide n. Note that $d \mid n$ is a **statement**, not a number: $2 \mid 6$ is *true*, it is not "2 divided by 6" and it is not 3. Likewise $10 \nmid 5$ is true, since $\frac{5}{10} \notin \mathbb{Z}$. Being a statement is what makes $2 \mid x$ a **predicate** — it acquires a truth value once x is fixed — so it is exactly the kind of thing a quantifier can be put in front of.

Divisibility inside a quantified statement

Two quantified divisibility statements, both **false**, both settled by a single counterexample — one counterexample is enough to make a $\forall$ statement false, though no single example could ever make one true (see quantified-statements[134] on that asymmetry):

Statement	Verdict	Counterexample
$\forall x \in \mathbb{Z}$, if $2 \mid x$ then $4 \mid x$	**False**	$x = 2$: $2 \mid 2$ is true but $4 \nmid 2$
$\forall x \in \mathbb{Z}$, if 6 is divisible by x, then $x = 2$	**False**	$x = 3$: $3 \in \mathbb{Z}$ and $3 \mid 6$, but $3 \neq 2$

A counterexample to a universal conditional has to make the **hypothesis true and the conclusion false** — that is what $\sim (p \to q) \equiv p \wedge \sim q$ says. An x that fails the hypothesis proves nothing.

The second statement becomes true once the conclusion lists every divisor:

$$\forall x \in \mathbb{Z},\ \text{if 6 is divisible by } x,\ \text{then } x = \pm 1 \text{ or } \pm 2 \text{ or } \pm 3 \text{ or } \pm 6.$$

The $\pm$ is not optional. The reason is in the definition: it asks only for $n = dk$ with $k \in \mathbb{Z}$, and k may be negative, so divisors over $\mathbb{Z}$ always come in $\pm$ pairs — if $n = dk$ then $n = (-d)(-k)$, so $d \mid n$ exactly when $(-d) \mid n$. A divisor list that quietly restricts itself to $\mathbb{Z}^+$ is answering a question about a different domain.

Proving and disproving divisibility statements

The pattern for a direct proof: unfold $d \mid n$ into $n = dk$, do algebra, then re-fold into the definition by exhibiting the integer witness.

$\forall a, b, c \in \mathbb{Z}$, if $c \mid a$ then $c \mid ab$.

> Let $a, b, c \in \mathbb{Z}$ and suppose $c \mid a$. Then $\exists k \in \mathbb{Z}$ such that $a = ck$. Multiplying both sides by b: $ab = ckb = c(kb)$. Since $k, b \in \mathbb{Z}$ we have $kb \in \mathbb{Z}$. Thus $c \mid ab$. $\square$

$\forall m \in \mathbb{Z}$, $6m(2m + 10m^2)$ is divisible by 4.

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

Let $m \in \mathbb{Z}$. Then $6m(2m+10m^2) = 2(3m)\cdot 2(m+5m^2) = 4(3m(m+5m^2))$. Since $m \in \mathbb{Z}$, $3m(m+5m^2) \in \mathbb{Z}$. Thus $4 \mid 6m(2m+10m^2)$. $\square$

$\forall a, b, c \in \mathbb{Z}$**, if** $a \mid (b+c)$ **then** $a \mid b$ **or** $a \mid c$ — **false**. Counterexample $a = 3, b = 4, c = 2$: $a \mid (b+c)$ since $3 \mid 6$, but $3 \nmid 4$ and $3 \nmid 2$.

$\forall a, b, m \in \mathbb{Z}$**, if** $m \mid (a+b)$ **then** $m \mid (a-b)$ — **false**. A counterexample needs the hypothesis true and the conclusion false:

	$m \mid (a+b)$	$m \mid (a-b)$	conditional
$m = 5, a = 20, b = 10$	$5 \mid 30$ T	$5 \mid 10$ T	T
$m = 5, a = 21, b = 13$	$5 \mid 34$ F	$5 \mid 8$ F	T
$m = 5, a = 27, b = 7$	$5 \mid 34$ F	$5 \mid 20$ T	T
$m = 5, a = 19, b = -9$	$5 \mid 10$ T	$5 \mid 28$ F	**F**
$m = 5, a = 23, b = 12$	$5 \mid 35$ T	$5 \mid 11$ F	**F**
$m = 5, a = -10, b = -3$	$5 \mid -13$ F	$5 \mid -7$ F	T

Only the two rows with hypothesis T and conclusion F are counterexamples.

$\forall m, n, q \in \mathbb{Z}$**, if** $m \mid n$ **and** $n \mid q$ **then** $m^2 \mid nq$ — **true**.

Let m, n, q be non-zero integers with $m \mid n$ and $n \mid q$. By definition there exist $a, b \in \mathbb{Z}$ with $n = ma$ and $q = nb$. Then

$$nq = (ma)(nb) = ma \cdot (mab) = m^2(a^2 b).$$

Since $a^2 b \in \mathbb{Z}$, we conclude $m^2 \mid nq$. $\square$

If k **is even and** m **is odd, then** $(k+2)^2 - (m-3)^2$ **is divisible by 4.**

Let $k = 2a$ and $m = 2b+1$ for some $a, b \in \mathbb{Z}$. Then $(k+2)^2 = (2a+2)^2 = 4(a+1)^2$ and $(m-3)^2 = (2b-2)^2 = 4(b-1)^2$, so

$$(k+2)^2 - (m-3)^2 = 4\big((a+1)^2 - (b-1)^2\big),$$

and $(a+1)^2 - (b-1)^2 \in \mathbb{Z}$. $\square$

$\forall c, d, e \in \mathbb{Z}$**, if** $c \mid d$ **and** $c \nmid e$**, then** $c \nmid (d+e)$**.**

Proof by contradiction. Suppose there exist integers c, d, e with $c \mid d$, $c \nmid e$ and $c \mid (d+e)$. Then $d = cx$ for some $x \in \mathbb{Z}$, and $d + e = cy$ for some $y \in \mathbb{Z}$. Hence $cx + e = cy$, so $e = c(y-x)$ with $y - x \in \mathbb{Z}$ — so $c \mid e$, a contradiction. $\square$

Every integer $n > 1$ is a product of primes

Proof by contradiction. Suppose the theorem is false. Then there exists an integer $n > 1$ that is not a product of primes. **Choose the smallest such** n — such a smallest one exists by the well-ordering principle. Choosing the smallest is what lets us assume every integer strictly between 1 and n *is* a product of primes.

Every integer $n > 1$ is either prime or composite (not both).

Case 1: n is prime. Then n is a product of primes (namely itself) — contradiction.

Case 2: n is composite. Then $n = rs$ for positive integers r, s with $r \neq 1$ and $s \neq 1$, which forces $1 < r < n$ and $1 < s < n$. Because n was chosen smallest, both r and s are products of primes, say $r = p_1 p_2 \cdots p_k$ and $s = q_1 q_2 \cdots q_\ell$. Therefore $n = rs = p_1 \cdots p_k q_1 \cdots q_\ell$ is a product of primes too.

Either way n is a product of primes, contradicting our choice of n. □

Unique Factorisation Theorem

Provided in the exam. This theorem and the Quotient-Remainder Theorem are both stated on the *MATH1061/MATH7861 Examination Formula Page*, so they can be cited rather than restated from memory — see also logical-equivalence-laws[135] for the rest of what that page carries.

Given any integer $n > 1$, the **standard factored form** of n is

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $k \in \mathbb{Z}^+$, the p_i are primes, the e_i are positive integers, and $p_1 < p_2 < \cdots < p_k$.

Both the primes and their exponents are unique — this is what makes the factored form a canonical fingerprint of an integer, and it's the engine behind divisor counting, gcd and lcm (see gcd-lcm-and-euclidean-algorithm[136]).

Counting divisors from the factorisation

Any positive divisor of $n = p_1^{e_1} \cdots p_k^{e_k}$ has the form $p_1^{a_1} \cdots p_k^{a_k}$ with $0 \leq a_i \leq e_i$, so there are

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

positive divisors.

[135] courses/math1061/logical-equivalence-laws.pdf
[136] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

$6975 = 3^2 \cdot 5^2 \cdot 31$, found by trial division: $6975 = 3 \cdot 2325 = 3 \cdot 3 \cdot 775 = 3 \cdot 3 \cdot 5 \cdot 155 = 3^2 \cdot 5^2 \cdot 31$. A divisor has 0, 1 or 2 threes; 0, 1 or 2 fives; and 0 or 1 thirty-ones — so $3 \cdot 3 \cdot 2 = 18$ positive divisors.

$27720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$**.**

$1400 = 2^3 \cdot 5^2 \cdot 7$, worked through:

- $1400 = 2(700) = 2 \cdot 2(350) = 2 \cdot 2(35)(10) = 2^2(5 \cdot 7)(2 \cdot 5) = 2^3 \cdot 5^2 \cdot 7^1$ — note the primes are written in increasing order.
- $1400^2 = (2^3 \cdot 5^2 \cdot 7)^2 = 2^6 \cdot 5^4 \cdot 7^2$ — raising to a power **multiplies** the exponents.
- $1400^3 = 1400 \cdot 1400^2 = 2^9 \cdot 5^6 \cdot 7^3$ — multiplying **adds** the exponents.
- Number of positive divisors of 1400: $(3 + 1)(2 + 1)(1 + 1) = 24$.
- Divisors of 1400 divisible by 8: all factors of the form $2^3 \cdot 5^* \cdot 7^*$, i.e. $8, 40, 200, 56, 280, 1400$.
- Smallest n with $1400n$ a perfect square: $1400n = t^2$ needs every exponent even. $t^2 = 2^3 \cdot 5^2 \cdot 7^1 \cdot n$, and splitting each power in half (bigger halves on the left) gives $t = 2^2 \cdot 5^1 \cdot 7^1$ against $2^1 \cdot 5^1 \cdot 7^0 \cdot n$, so $n = 2 \cdot 7 = 14$.

Primality testing

Lemma: for every integer $n > 1$, if no integer x in the range $1 < x \leq \sqrt{n}$ divides n, then n is prime.

This is why trial division only has to go as far as $\sqrt{n}$ — for 6975, only up to $\sqrt{6975} = 83.51\ldots$

> *Proof by contraposition.* The contrapositive is: $\forall n \in \mathbb{Z}^{\geq 2}$, if n is not prime, then there exists an integer x with $1 < x \leq \sqrt{n}$ such that $x \mid n$.
>
> Suppose $n \in \mathbb{Z}^{\geq 2}$ and n is not prime. Then n is composite, so by definition $\exists r, s \in \mathbb{Z}^+$ with $n = rs$ and $1 < r < n$ and $1 < s < n$.
>
> *Case 1:* $r = s$. Then $r = s = \sqrt{n}$.
>
> *Case 2:* $r \neq s$. Then one of r, s is less than $\sqrt{n}$ and the other greater — if both were greater we'd have $rs > n$, and if both were less we'd have $rs < n$.
>
> In either case there is an $x \in \{r, s\}$ with $1 < x \leq \sqrt{n}$ and $x \mid n$. $\square$

There are infinitely many primes

Lemma: for any integer a and any prime p, if $p \mid a$ then $p \nmid (a + 1)$.

Proof by contradiction. Let $a \in \mathbb{Z}$, let p be prime, suppose $p \mid a$, and assume for a contradiction that $p \mid (a+1)$. Since $p \mid a$ there exists $k \in \mathbb{Z}$ with $a = pk$; since $p \mid (a+1)$ there exists $\ell \in \mathbb{Z}$ with $a + 1 = p\ell$. So

$$1 = (a+1) - a = p\ell - pk = p(\ell - k),$$

and $\ell - k \in \mathbb{Z}$, so $p \mid 1$. But $p \geq 2$ for any prime, whereas $p \mid 1$ forces $p = \pm 1$ — a contradiction. □

Theorem: there are an infinite number of primes.

Proof by contradiction. Suppose the number of primes is finite. Then some prime p is the largest, and we can list every prime in ascending order: $2, 3, 5, 7, 11, \ldots, p$.

Let $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$.

Then $N > 1$, so by the Unique Factorisation Theorem N is a product of primes and hence divisible by some prime q. Because q is prime it must be one of $2, 3, 5, 7, 11, \ldots, p$.

So q divides $2 \cdot 3 \cdot 5 \cdots p$ — that is, $q \mid (N-1)$ — and hence by the lemma $q \nmid ((2 \cdot 3 \cdot 5 \cdots p) + 1) = N$.

So q divides N and q does not divide N: a contradiction. Therefore the original statement is true. □

See also

- proof-techniques[137] · modular-arithmetic[138] · gcd-lcm-and-euclidean-algorithm[139]
- partial-order-relations[140] — "divides" as a partial order on $\mathbb{Z}^+$
- fields[141] — unique factorisation as the reason $\mathbb{Z}_p$ is a field when p is prime
- counting-principles[142] — the rule behind counting divisors, one choice of exponent for each prime
- practice-problems[143] — §13 Divisibility, with full worked solutions

[137] courses/math1061/proof-techniques.pdf
[138] courses/math1061/modular-arithmetic.pdf
[139] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[140] courses/math1061/partial-order-relations.pdf
[141] courses/math1061/fields.pdf
[142] courses/math1061/counting-principles.pdf
[143] courses/math1061/practice-problems.pdf

Equivalence Classes and Partitions

An equivalence relation sorts its set into groups of mutually related elements, the **equivalence classes**. The classes cut the set into non-overlapping pieces, a **partition**, and every partition comes from an equivalence relation in this way. Equivalence relations themselves are in equivalence-relations[144]. First met in 2026-09-21-equivalence-relations[145], and finished at the start of 2026-09-22-partial-order-relations[146].

The definition

> Let ρ be an equivalence relation on a set S. For each $a \in S$, define the **equivalence class** of a by
>
> $$[a] = \{x \in S : x \ \rho \ a\}$$
>
> (the set of elements related to a).

Three things to read off the definition:

- $[a]$ **is a set**, a subset of S. It is not an element of S, and it is not a number.
- $a \in [a]$ **always**, because ρ is reflexive. So no class is empty.
- **The bracket depends on the relation.** $[1]$ means one thing for congruence mod 3 and another for $x - y \in \mathbb{Q}$. Say which relation is meant.

Relation	Class	As a set
$m \equiv n \pmod 3$ on $\mathbb{Z}$	$[1]$	$\{\dots, -5, -2, 1, 4, 7, \dots\}$
same parity on $\mathbb{Z}$	$[0]$	$\mathbb{Z}^{even}$
$x - y \in \mathbb{Q}$ on $\mathbb{R}$	$[1]$	$\mathbb{Q}$
$x - y \in \mathbb{Q}$ on $\mathbb{R}$	$[\sqrt{2}]$	$\{y + \sqrt{2} : y \in \mathbb{Q}\}$
same part of $\{\{1,2,3\},\{4,5\},\{6\}\}$	$[4]$	$\{4, 5\}$

Describing a class

To find $[a]$, ask **which x are related to a**: write down $x \ \rho \ a$, unfold the definition of ρ, and simplify until it is a plain condition on x.

$[1]$ **for $x \ \tau \ y \leftrightarrow x - y \in \mathbb{Q}$.** A real y is related to 1 exactly when $1 - y \in \mathbb{Q}$, which happens exactly when $y \in \mathbb{Q}$. So $[1] = \mathbb{Q}$.

[144] courses/math1061/equivalence-relations.pdf
[145] courses/math1061/2026-09-21-equivalence-relations.pdf
[146] courses/math1061/2026-09-22-partial-order-relations.pdf

$[\sqrt{2}]$ **for the same relation.** $x \tau \sqrt{2}$ means $x - \sqrt{2} = y$ for some $y \in \mathbb{Q}$, that is, $x = y + \sqrt{2}$. So $[\sqrt{2}] = \{y + \sqrt{2} : y \in \mathbb{Q}\}$. It contains $\sqrt{2}$, $1 + \sqrt{2}$, $-3 + \sqrt{2}$, and so on.

$[1]$ **for** $m \sigma n \leftrightarrow 8 \mid (m - n)$ **or** $8 \mid (m + n)$**.**

$$[1] = \{n \in \mathbb{Z} : 8 \mid (1 - n) \text{ or } 8 \mid (1 + n)\} = \{n \in \mathbb{Z} : n \equiv 1 \text{ or } 7 \pmod 8\}.$$

The second alternative says $n \equiv -1 \pmod 8$, and $-1 \equiv 7$. All five classes of σ are in 2026-09-22-partial-order-relations[147].

These three are worked in 2026-09-21-equivalence-relations[148] and 2026-09-22-partial-order-relations[149]. The definition has $x \rho a$ and the workings sometimes use $a \rho x$. For an equivalence relation the two say the same thing, by symmetry.

When the class is infinite, describe it by a condition, as above. Listing "$\{\dots, -7, -1, 1, 7, 9, \dots\}$" is a useful check, but the pattern has to be stated.

One class, many names

For congruence mod 3,

$$[0] = [3] = [-6].$$

These are three names for one set, $\{\dots, -6, -3, 0, 3, 6, \dots\}$. The element inside the bracket is a **representative** of the class, and **every element of a class is a representative of it**. The rule for when two names give the same class is:

$[a] = [b]$ **if and only if** $a \rho b$**.**

So to decide whether two classes are equal, test the two representatives against each other. For example, is $[\sqrt{2}] = [-\sqrt{2}]$ for τ? $\sqrt{2} - (-\sqrt{2}) = 2\sqrt{2} \notin \mathbb{Q}$, so $\sqrt{2} \not\tau -\sqrt{2}$, and $[\sqrt{2}] \neq [-\sqrt{2}]$.

The rule follows from the result in the next section: if $a \rho b$ the classes are equal, and if $a \not\rho b$ they are disjoint and non-empty, so not equal. By convention the simplest representative is used. For congruence mod n the usual choice is $[0], [1], \dots, [n-1]$ (integers-modulo-n[150]).

Equal or disjoint

> **Important result.** If ρ is an equivalence relation on a set S, and $a, b \in S$, then either
>
> $$[a] = [b] \qquad \text{or} \qquad [a] \cap [b] = \emptyset.$$
>
> If $a \rho b$ the classes are equal. If $a \not\rho b$ they are disjoint.

[147] courses/math1061/2026-09-22-partial-order-relations.pdf
[148] courses/math1061/2026-09-21-equivalence-relations.pdf
[149] courses/math1061/2026-09-22-partial-order-relations.pdf
[150] courses/math1061/integers-modulo-n.pdf

Two classes never partly overlap. The proof uses each of the three properties.

Proof. Let ρ be an equivalence relation on S and let $a, b \in S$.

Case 1: $a \rho b$. We show $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Let $x \in [a]$. Then $x \rho a$. Since also $a \rho b$, **transitivity** gives $x \rho b$, so $x \in [b]$. Hence $[a] \subseteq [b]$. By **symmetry**, $b \rho a$, and the same argument with a and b exchanged gives $[b] \subseteq [a]$. Hence $[a] = [b]$.

Case 2: $a \not\rho b$. Suppose, for a contradiction, that $[a] \cap [b] \neq \emptyset$, and take $x \in [a] \cap [b]$. Then $x \rho a$ and $x \rho b$. By **symmetry**, $a \rho x$. By **transitivity**, $a \rho x$ and $x \rho b$ give $a \rho b$. ($\Rightarrow\Leftarrow$) Hence $[a] \cap [b] = \emptyset$. $\square$

Reflexivity is what puts a into $[a]$. It gives *if* $[a] = [b]$ *then* $b \in [a]$ in one line: $b \in [b] = [a]$.

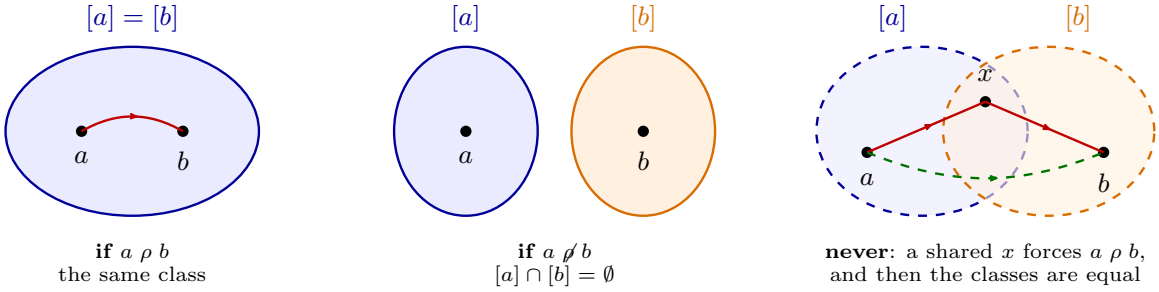


Figure 30: The two things that can happen to two equivalence classes, and the one that cannot. Left: if $a \rho b$ then $[a]$ and $[b]$ are the same set. Middle: if a and b are not related then the two classes share no element. Right: a partial overlap is impossible. A shared element x is related to both a and b; symmetry turns $x \rho a$ round into $a \rho x$, and transitivity along $a \to x \to b$ then forces $a \rho b$, the dashed arrow, which puts the pair back in the left-hand picture.

Putting the pieces together, for an equivalence relation ρ these four statements stand or fall together:

$$a \rho b \qquad [a] = [b] \qquad b \in [a] \qquad [a] \cap [b] \neq \emptyset$$

Partitions

Two sets X and Y are **disjoint** if and only if $X \cap Y = \emptyset$.
A collection of sets is **mutually disjoint** if each pair of distinct sets in the collection is disjoint.
A **partition** of a set S is a collection of non-empty and mutually disjoint subsets of S whose union is S. The subsets in a partition are sometimes called **parts**.

So a collection of subsets of S is a partition when it passes three checks:

1. every part is **non-empty**;
2. the parts are **mutually disjoint**: no element is in two of them;
3. their **union is** S: no element is left out.

Checks 2 and 3 together say that **every element of S is in exactly one part**. The same definition, in Lecture 17's words and with more worked examples, is in sets-and-set-notation[151].

Mutually disjoint is about pairs. $W = \{1, 2, 3\}$, $X = \{4, 5, 6\}$, $Y = \{6, 7, 8\}$ are not mutually disjoint, because $X \cap Y = \{6\}$, even though W is disjoint from both of the others. More examples are in 2026-09-21-equivalence-relations[152].

The classes form a partition

> The equivalence classes of an equivalence relation on a set S form a partition of the set S.

The three checks, for the collection of all classes $\{[a] : a \in S\}$:

1. **Non-empty.** $a \in [a]$, by reflexivity.
2. **Mutually disjoint.** Two *distinct* classes are not equal, so by the result above they are disjoint.
3. **Union is S.** Each $a \in S$ lies in the class $[a]$, and every class is a subset of S.

In the collection each class is counted once, however many names it has. For congruence mod 3 the collection is $\{[0], [1], [2]\}$, with three members, although $[0] = [3] = [-6] = \cdots$.

Relation	Number of classes
$m \equiv n \pmod 3$ on $\mathbb{Z}$	3
same parity on $\mathbb{Z}$	2
$8 \mid (m - n)$ or $8 \mid (m + n)$ on $\mathbb{Z}$	5
$x - y \in \mathbb{Q}$ on $\mathbb{R}$	infinitely many
$x = y$ on a set S	one for each element of S

[151] courses/math1061/sets-and-set-notation.pdf
[152] courses/math1061/2026-09-21-equivalence-relations.pdf

From a partition to a relation

> Given any partition of a set S, we can define an equivalence relation on S, by defining two elements to be related if and only if they are in the same part of the partition. The parts in a partition form the equivalence classes of the corresponding equivalence relation.

"In the same part" is an equivalence relation. The check is short, and it shows what each condition on a partition is for.

- **Reflexive.** Let $x \in S$. The union of the parts is S, so x is in some part, and it is in the same part as itself.
- **Symmetric.** If x and y are in the same part, then y and x are.
- **Transitive.** Suppose x and y are both in a part P, and y and z are both in a part Q. Then $y \in P \cap Q$. The parts are mutually disjoint, so P and Q cannot be distinct: $P = Q$. So x and z are in the same part.

Reflexivity uses "the union is S", and transitivity uses "mutually disjoint".

Writing the relation down. For a small set, list the pairs: a part with k elements gives all k^2 ordered pairs of its elements. The partition $\{\{1,2,3\},\{4,5\},\{6\}\}$ of $\{1,\dots,6\}$ gives $9+4+1=14$ pairs, drawn in 2026-09-21-equivalence-relations[153]. For an infinite set, turn "in the same part" into a condition. For the partition $\{\mathbb{Z}^-,\{0\},\mathbb{Z}^+\}$ of $\mathbb{Z}$ the condition is

$$a \tau b \longleftrightarrow a, b \text{ both positive} \quad \text{or} \quad a = b = 0 \quad \text{or} \quad a, b \text{ both negative}$$

with one alternative for each part (2026-09-22-partial-order-relations[154]).

Two descriptions of one thing

> Any partition defines an equivalence relation and any equivalence relation defines a partition.

In short, **equivalence relations** $\iff$ **partitions**. The two constructions undo each other:

- Start with an equivalence relation, take its classes, and relate elements in the same class. That gives back the relation you started with, since $x \rho y$ exactly when $[x] = [y]$.
- Start with a partition, relate elements in the same part, and take the classes. That gives back the parts.

[153] courses/math1061/2026-09-21-equivalence-relations.pdf
[154] courses/math1061/2026-09-22-partial-order-relations.pdf

So an equivalence relation on S and a partition of S carry the same information. A question about one can be answered with the other. To count or describe the equivalence relations on a small set, describe its partitions. To show a collection of sets is a partition, it is enough to recognise it as the classes of an equivalence relation.

Finding the classes of a finite relation

For an equivalence relation given by a list of pairs or an arrow diagram:

1. Pick any element a. Its class is a together with everything joined to a by an arrow.
2. Pick any element not yet in a class, and do the same.
3. Stop when every element is in a class.

Step 1 is the definition of $[a]$, so it collects the whole class at once. There is no need to follow arrows further, because the relation is transitive. Step 2 starts a new class because, by the equal-or-disjoint result, an element outside the classes found so far has a class disjoint from all of them.

Worked (practice-problems[155], Q2). On $A = \{a, b, c, d, e\}$,

$$\rho = \{(a,a),(a,b),(a,d),(b,b),(c,c),(d,d),(b,a),(d,a),(b,d),(d,b),(c,e),(e,c),(e,e)\}.$$

Start at a: it is related to a, b, d, so $[a] = \{a, b, d\}$. The first unused element is c: it is related to c and e, so $[c] = \{c, e\}$. Every element is used, and

$$[a] = [b] = [d] = \{a, b, d\}, \qquad [c] = [e] = \{c, e\}.$$

The same problem asks for the smallest equivalence relation contained in ρ. A relation on A must contain all five loops to be reflexive, and the five loops alone are already an equivalence relation: $\tau = \{(a,a),(b,b),(c,c),(d,d),(e,e)\}$, which is equality on A. Its classes are the five singletons.

Common mistakes

- **Treating $[a]$ as an element.** $[a] \subseteq S$, and $a \in [a]$. Writing $[a] \in S$ or $[1] = 1$ confuses a set with one of its members (sets-and-set-notation[156]).
- **Thinking different names mean different classes.** $[0]$ and $[3]$ are the same class mod 3. $a \neq b$ does not give $[a] \neq [b]$. Only $a \not\sim b$ does.
- **Giving one example in place of the class.** "$[\sqrt{2}]$ contains $1 + \sqrt{2}$" does not describe $[\sqrt{2}]$. $\{y + \sqrt{2} : y \in \mathbb{Q}\}$ does.

[155] courses/math1061/practice-problems.pdf
[156] courses/math1061/sets-and-set-notation.pdf

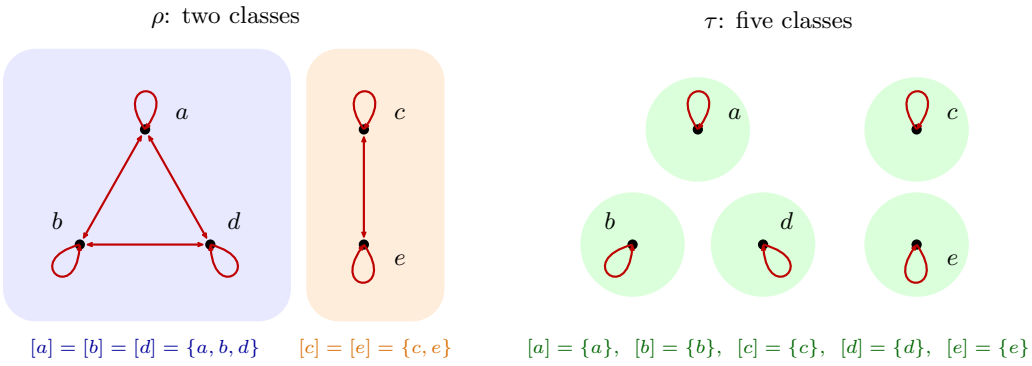


Figure 31: Two equivalence relations on a, b, c, d, e, with each class shaded. Left: ρ has 13 pairs, 9 inside a, b, d and 4 inside c, e. A double-headed line stands for an arrow each way. Its classes are the two clusters of the diagram. Right: τ keeps only the five loops. It is still reflexive, symmetric and transitive, and each element is in a class by itself. Here τ is contained in ρ, and the smaller relation has more, smaller classes.

- **Classes that overlap or leave something out.** If your list of classes is not a partition of S, something is wrong. Check that each element is in exactly one.
- **Taking classes of a relation that is not an equivalence relation.** The definition starts "let ρ be an equivalence relation". For $x + y \in \mathbb{Q}$ on $\mathbb{R}$, the set of things related to $\sqrt{2}$ does not even contain $\sqrt{2}$.
- **An empty part.** $\{\emptyset, \mathbb{Z}\}$ is not a partition of $\mathbb{Z}$. Parts are non-empty.

See also

- equivalence-relations[157] — the definition, the proof template, and the relations used here
- sets-and-set-notation[158] — partitions as first defined, with more examples
- integers-modulo-n[159] — the classes of congruence mod n as a number system
- counting-principles[160] — the size of a finite set as the sum of the sizes of the parts of a partition
- reflexive-symmetric-and-transitive-relations[161] — the three properties the proofs here use
- proof-techniques[162] — double containment and proof by contradiction, both used in the equal-or-disjoint proof

[157] courses/math1061/equivalence-relations.pdf
[158] courses/math1061/sets-and-set-notation.pdf
[159] courses/math1061/integers-modulo-n.pdf
[160] courses/math1061/counting-principles.pdf
[161] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[162] courses/math1061/proof-techniques.pdf

- 2026-09-21-equivalence-relations[163] — Lecture 24 · 2026-09-22-partial-order-relations[164] — Lecture 25, which finishes it
- practice-problems[165] — §31, with full worked solutions

Equivalence Relations

A relation that is reflexive, symmetric and transitive at once. Such a relation behaves like "is the same as, in some respect", and it sorts its set into groups, the equivalence classes of equivalence-classes-and-partitions[166]. The three properties are in reflexive-symmetric-and-transitive-relations[167]. First met in 2026-09-21-equivalence-relations[168].

The definition

> A relation is an **equivalence relation** if and only if it is: reflexive, symmetric and transitive.

For a relation ρ on a set A that is three "for all" statements:

(1) reflexive: $\forall x \in A,\ x\ \rho\ x$.

(2) symmetric: $\forall x, y \in A,\ x\ \rho\ y \to y\ \rho\ x$.

(3) transitive: $\forall x, y, z \in A,\ (x\ \rho\ y \text{ and } y\ \rho\ z) \to x\ \rho\ z$.

All three are needed, and none follows from the other two (reflexive-symmetric-and-transitive-relations[169]).

Relations here are named ρ, τ, σ, R and T. The symbol $\sim$ is also used as the name of a relation, as in $(a, b) \sim (c, d)$. It is the same symbol used for *not* in logic (logical-connectives[170]). Position tells them apart: between two objects it is a relation, and in front of a statement it is a negation.

[163] courses/math1061/2026-09-21-equivalence-relations.pdf
[164] courses/math1061/2026-09-22-partial-order-relations.pdf
[165] courses/math1061/practice-problems.pdf
[166] courses/math1061/equivalence-classes-and-partitions.pdf
[167] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[168] courses/math1061/2026-09-21-equivalence-relations.pdf
[169] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[170] courses/math1061/logical-connectives.pdf

What the arrow diagram looks like

In the arrow diagram of an equivalence relation every dot has a loop, every arrow has its return, and every two-step path has its short cut. Put together, the diagram falls into **separate clusters, with every possible arrow inside a cluster and none between clusters**. The clusters are the equivalence classes. The even integers under *same parity* are a single such cluster (2026-09-21-equivalence-relations[171]). The same shape shows for five real numbers in 2026-09-21-equivalence-relations[172], and for congruence mod 6 in relations-on-sets[173].

Figure 32 shows the shape, and one way to break each property.

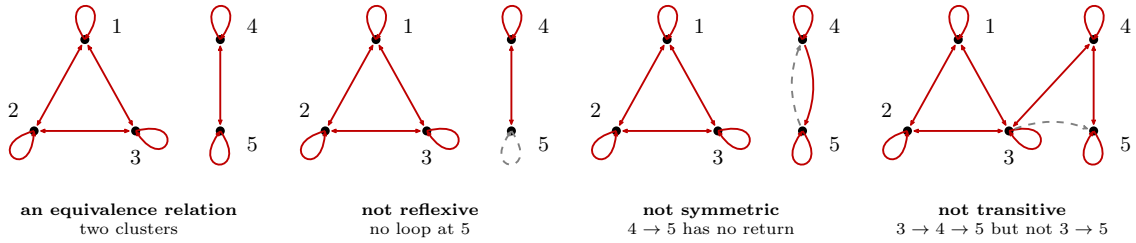


Figure 32: An equivalence relation on $1, 2, 3, 4, 5$ and three near misses, each differing from it in one place. A double-headed line stands for an arrow each way, and what is missing is dashed. First: two clusters, complete inside, nothing between them. Second: the loop at 5 is removed, so the relation is not reflexive. Third: $5 \to 4$ is removed, so $4 \to 5$ has no return and the relation is not symmetric. Fourth: a link between 3 and 4 is added, so the path $3 \to 4 \to 5$ has no short cut $3 \to 5$ and the relation is not transitive. A link between two clusters has to be completed until they are one cluster, or removed.

Proving a relation is an equivalence relation

Prove the three properties one at a time, and label each part. Each part is a direct proof of a "for all" statement (proof-techniques[174]):

Part	Start with	Show
reflexive	Let $x \in A$.	$x \rho x$
symmetric	Let $x, y \in A$ and suppose $x \rho y$.	$y \rho x$

[171] courses/math1061/2026-09-21-equivalence-relations.pdf
[172] courses/math1061/2026-09-21-equivalence-relations.pdf
[173] courses/math1061/relations-on-sets.pdf
[174] courses/math1061/proof-techniques.pdf

Part	Start with	Show
transitive	Let $x, y, z \in A$ and suppose $x \rho y$ and $y \rho z$.	$x \rho z$

In each part, **unfold** what ρ means for the elements in hand, work with that, and **fold** it back into a statement about ρ. Finish with a sentence naming all three: *Since ρ is reflexive, symmetric and transitive, it is an equivalence relation.*

Worked: $x \tau y \leftrightarrow x - y \in \mathbb{Q}$ on $\mathbb{R}$

The proof is written out in full in 2026-09-21-equivalence-relations[175]. Its shape:

- **Reflexive.** $x - x = 0 \in \mathbb{Q}$.
- **Symmetric.** Unfold $x - y \in \mathbb{Q}$ to $x - y = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$. Then $y - x = \frac{-a}{b} \in \mathbb{Q}$.
- **Transitive.** Unfold to $x - y = \frac{a}{b}$ and $y - z = \frac{c}{d}$. Then $x - z = (x - y) + (y - z) = \frac{ad+bc}{bd} \in \mathbb{Q}$, with $bd \neq 0$.

The second fraction gets **new letters** c, d. The transitive step rests on one identity, $x - z = (x - y) + (y - z)$, which gets rid of the middle element. Most transitivity proofs need a step like it.

Congruence is the same proof with integers in place of rationals. $m \rho n \leftrightarrow d \mid (m - n)$ on $\mathbb{Z}$ is worked for $d = 6$ in reflexive-symmetric-and-transitive-relations[176], and nothing in it depends on the 6.

Worked: a definition with an "or"

$m \sigma n \leftrightarrow (8 \mid (m - n))$ or $(8 \mid (m + n))$ on $\mathbb{Z}$.

The proof is written out in full in 2026-09-21-equivalence-relations[177]. When the definition is an *or*, every hypothesis of the form $m \sigma n$ splits into cases, and each case has to reach the conclusion. A conclusion of the form $k \sigma n$ needs only **one** of its two alternatives.

- **Reflexive.** No cases: $8 \mid (m - m)$, the first alternative.
- **Symmetric.** One hypothesis, two cases. From $8 \mid (m - n)$ get $8 \mid (n - m)$. From $8 \mid (m + n)$ get $8 \mid (n + m)$.
- **Transitive.** Two hypotheses, $2 \times 2 = 4$ cases:

[175] courses/math1061/2026-09-21-equivalence-relations.pdf
[176] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[177] courses/math1061/2026-09-21-equivalence-relations.pdf

Case	$k \sigma m$ because	$m \sigma n$ because	Combine	So 8 divides
1	$8 \mid (k-m)$	$8 \mid (m-n)$	add	$k-n$
2	$8 \mid (k-m)$	$8 \mid (m+n)$	add	$k+n$
3	$8 \mid (k+m)$	$8 \mid (m-n)$	subtract	$k+n$
4	$8 \mid (k+m)$	$8 \mid (m+n)$	subtract	$k-n$

In every row the two quantities are added or subtracted, whichever cancels the m.

Disproving

A relation fails to be an equivalence relation as soon as it fails **one** of the three properties, and a property fails as soon as there is **one** witness. So a disproof is short: name the property, give specific elements, check them.

> $x \rho y \leftrightarrow x + y \in \mathbb{Q}$ on $\mathbb{R}$ is not an equivalence relation: it is not reflexive, because $\sqrt{2} + \sqrt{2} = 2\sqrt{2} \notin \mathbb{Q}$, so $\sqrt{2} \not\rho \sqrt{2}$.

That is the whole answer (2026-09-21-equivalence-relations[178]). Try reflexivity first, since it involves only one element. A relation can fail on any of the three:

Fails	Relation	Witness	Worked in
reflexive	$x + y \in \mathbb{Q}$ on $\mathbb{R}$	$\sqrt{2} \not\rho \sqrt{2}$	2026-09-21-equivalence-relations[179]
symmetric	x is a multiple of y, on $\mathbb{Z}$	4 is a multiple of 2, but 2 is not a multiple of 4	practice-problems[180], Q1 (β)
transitive	$\lvert x-y\rvert \leq 1$ on $\mathbb{Z}$	0 and 1 are related, 1 and 2 are related, 0 and 2 are not	—

The last one is reflexive and symmetric, and still not an equivalence relation. "Close to" is not transitive, and that is why it never works as a kind of sameness.

[178] courses/math1061/2026-09-21-equivalence-relations.pdf
[179] courses/math1061/2026-09-21-equivalence-relations.pdf
[180] courses/math1061/practice-problems.pdf

"The same …"

Most of the course's equivalence relations say that two elements have **the same** something:

Relation	x and y are related when they have the same …
$m \equiv n \pmod 3$ on $\mathbb{Z}$	remainder on division by 3
same parity on $\mathbb{Z}$	parity
in the same part of a partition	part
$(a,b) \sim (c,d) \leftrightarrow ad = bc$	value as a fraction
R_n on strings	first n characters (practice-problems[181], Q3)
$x = y$ on any set	identity

A relation of the form "x and y have the same value of f", that is $f(x) = f(y)$ for some function f on the set, is always an equivalence relation, because the three properties are inherited from $=$: $f(x) = f(x)$; if $f(x) = f(y)$ then $f(y) = f(x)$; and if $f(x) = f(y)$ and $f(y) = f(z)$ then $f(x) = f(z)$. Recognising this shape tells you the answer is *yes* before you start. The proof still has to be written out for the relation as given.

Not every example is given in that form. $x - y \in \mathbb{Q}$ and the relation σ above have to be proved from their definitions.

The same fraction

An equivalence relation that is neither congruence nor equality:

$$(a,b) \sim (c,d) \text{ if and only if } ad = bc$$

The set is $\mathbb{Z}^+ \times \mathbb{Z}^+$, pairs of positive integers, with (a,b) standing for the fraction $\frac{a}{b}$. Two pairs are related when cross-multiplying gives equal products. The condition $ad = bc$ says $\frac{a}{b} = \frac{c}{d}$ without dividing, so it stays inside the integers. For example $\frac{1}{2} = \frac{2}{4} = \frac{3}{6}$, so $(1,2)$, $(2,4)$ and $(3,6)$ are all related.

- **Reflexive.** Let $(a,b) \in \mathbb{Z}^+ \times \mathbb{Z}^+$. Then $ab = ba$, so $(a,b) \sim (a,b)$.
- **Symmetric.** Suppose $(a,b) \sim (c,d)$, so $ad = bc$. Then $cb = da$, so $(c,d) \sim (a,b)$.
- **Transitive.** Suppose $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$, so $ad = bc$ and $cf = de$. Then

  $$(af)d = (ad)f = (bc)f = b(cf) = b(de) = (be)d,$$

  and since $d \neq 0$ we may cancel it: $af = be$. So $(a,b) \sim (e,f)$.

Each equivalence class is one positive rational number, with all the ways of writing it: $[(1,2)] = \{(1,2),(2,4),(3,6),\dots\}$. So the positive rationals $\mathbb{Q}^+$ can be built as the classes of this relation. The figure below draws the classes as rays.

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

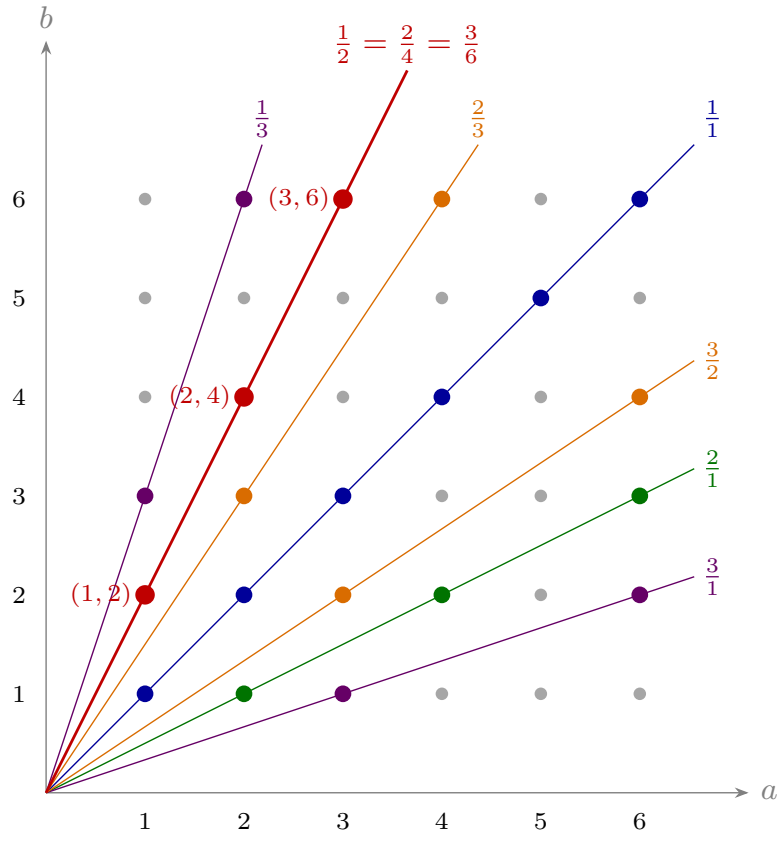


Figure 33: The pairs (a, b) with a and b from 1 to 6, plotted as points. Two pairs satisfy $ad = bc$ exactly when they lie on the same line through the origin, so the equivalence classes are the rays out of the origin, and each ray is one positive rational. The red ray holds $(1, 2)$, $(2, 4)$ and $(3, 6)$, the three fractions of $\frac{1}{2} = \frac{2}{4} = \frac{3}{6}$. Six more rays are coloured and labelled with their fraction. Every grey point is on a ray of its own within this window.

The examples side by side

Relation	on	Equivalence relation?	Classes
$m \equiv n \pmod 3$	$\mathbb{Z}$	**yes**	[0], [1], [2]
same parity	$\mathbb{Z}$	**yes**	$\mathbb{Z}^{even}$, $\mathbb{Z}^{odd}$
$x - y \in \mathbb{Q}$	$\mathbb{R}$	**yes**	$[a] = \{y + a : y \in \mathbb{Q}\}$, infinitely many
$8 \mid (m - n)$ or $8 \mid (m + n)$	$\mathbb{Z}$	**yes**	five: [0], [1], [2], [3], [4]
in the same part of $\{\{1,2,3\},\{4,5\},\{6\}\}$	$\{1, \ldots, 6\}$	**yes**	the three parts
$ad = bc$	$\mathbb{Z}^+ \times \mathbb{Z}^+$	**yes**	one for each positive rational
$x = y$	any set	**yes**	one for each element, $[a] = \{a\}$
$3 \mid (x^2 - y^2)$	$\mathbb{Z}$	**yes**	multiples of 3, non-multiples of 3
$x + y \in \mathbb{Q}$	$\mathbb{R}$	no, not reflexive	—
x is a multiple of y	$\mathbb{Z}$	no, not symmetric	—

The classes for the first five rows and the ninth are worked in equivalence-classes-and-partitions[182]. The eighth and tenth are γ and β of practice-problems[183], Q1.

Common mistakes

- **Proving two properties and stopping**, or checking a property on a few examples. Each property is a "for all", and needs a general argument about arbitrary elements.
- **Assuming the conclusion in the symmetric part.** The hypothesis is only $x \rho y$. $y \rho x$ is what has to come out.
- **Reusing a letter when unfolding twice.** $x - y = \frac{a}{b}$ and $y - z = \frac{a}{b}$ would say the two differences are equal. Use $\frac{c}{d}$.
- **Skipping reflexivity because "symmetric and transitive give it".** They do not (reflexive-symmetric-and-transitive-relations[184]).
- **Disproving without a witness.** "It isn't always true that $x + x$ is rational" is not a disproof. $x = \sqrt{2}$ is.
- **Forgetting the set.** The same rule on a different set is a different relation. $x + y \in \mathbb{Q}$ fails on $\mathbb{R}$, but on $\mathbb{Q}$ every pair is related and it is an equivalence relation with a single class.

[182] courses/math1061/equivalence-classes-and-partitions.pdf
[183] courses/math1061/practice-problems.pdf
[184] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf

See also

- equivalence-classes-and-partitions[185] — the classes of an equivalence relation, and why they partition the set
- reflexive-symmetric-and-transitive-relations[186] — the three properties, one at a time
- relations-on-sets[187] — relations as sets of pairs, and arrow diagrams
- partial-order-relations[188] — the other important kind of relation, with antisymmetric in place of symmetric
- modular-arithmetic[189] · integers-modulo-n[190] — congruence, and its classes as the elements of $\mathbb{Z}_n$
- rational-and-irrational-numbers[191] — the definition of rational that the $x - y \in \mathbb{Q}$ proof unfolds
- 2026-09-21-equivalence-relations[192] — Lecture 24
- practice-problems[193] — §31, with full worked solutions

Groups

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[194], and the bijections of the symmetric-group[195] under composition. A small group is checked from its table (cayley-tables[196]). Groups inside groups, and the powers of an element, are in subgroups-and-cyclic-groups[197]. First met in 2026-09-24-definitions-and-examples-of-groups[198], and continued in 2026-10-06-elementary-properties-of-groups[199].

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:-

[185] courses/math1061/equivalence-classes-and-partitions.pdf
[186] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[187] courses/math1061/relations-on-sets.pdf
[188] courses/math1061/partial-order-relations.pdf
[189] courses/math1061/modular-arithmetic.pdf
[190] courses/math1061/integers-modulo-n.pdf
[191] courses/math1061/rational-and-irrational-numbers.pdf
[192] courses/math1061/2026-09-21-equivalence-relations.pdf
[193] courses/math1061/practice-problems.pdf
[194] courses/math1061/integers-modulo-n.pdf
[195] courses/math1061/symmetric-group.pdf
[196] courses/math1061/cayley-tables.pdf
[197] courses/math1061/subgroups-and-cyclic-groups.pdf
[198] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[199] 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[200]).
- **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.

[200] 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[201]).

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.

[201] 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[202], 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[203])? All eight against all four properties:

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

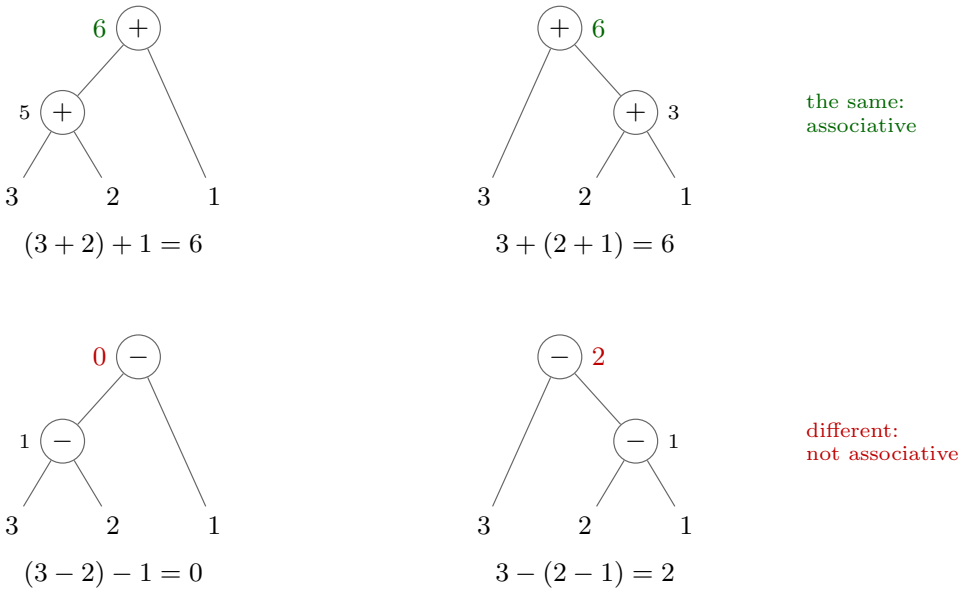


Figure 34: The two ways of bracketing three elements, drawn as trees: the lower operation is done first, and its result feeds the upper one. Top row, addition: both bracketings of $3+2+1$ give 6. Addition is associative, so the brackets can be dropped. Bottom row, subtraction: $(3-2)-1=0$ and $3-(2-1)=2$. 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[204]: $[1]^{-1} = [1]$, $[2]^{-1} = [3]$, $[3]^{-1} = [2]$, $[4]^{-1} = [4]$.

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[205].

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[206]). 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)

[204] courses/math1061/practice-problems.pdf
[205] courses/math1061/integers-modulo-n.pdf
[206] 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[207], proved in 2026-09-24-definitions-and-examples-of-groups[208]).
- **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.

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

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

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.

A check in S_3 (symmetric-group[209]). $f_2 \circ f_3 = f_6$, 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

[209] courses/math1061/symmetric-group.pdf

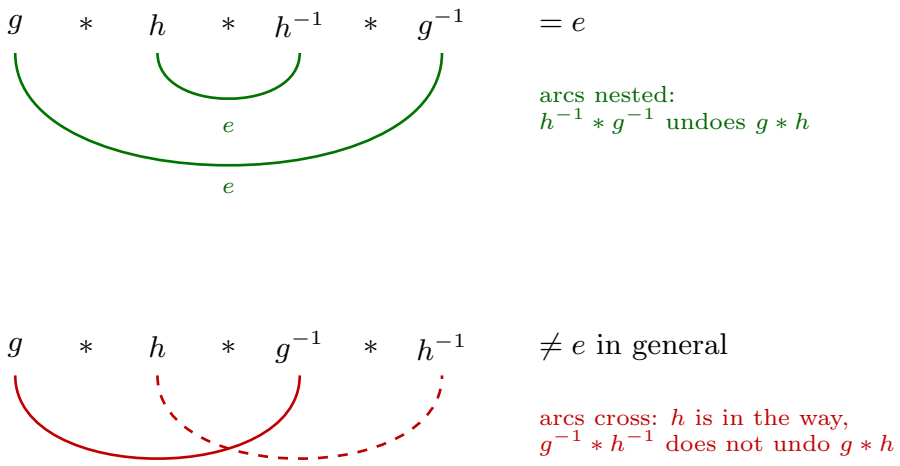


Figure 35: Why the inverse of $g * h$ is $h^{-1} * g^{-1}$ and not $g^{-1} * h^{-1}$. Top: in $g * h * h^{-1} * g^{-1}$ each element sits next to its inverse once the inner pair is gone. The inner arc, $h * h^{-1} = e$, cancels first, and that brings g next to g^{-1}, so the whole product is e. The arcs 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.

$f_2^{-1} \circ f_3^{-1} = f_2 \circ f_3 = f_6$, 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[210]).

The inverse facts are Q2 of practice-problems[211].

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[212] — a finite group as a table, and what can be read off it
- integers-modulo-n[213] — $\mathbb{Z}_n$ under addition, and $\mathbb{Z}_n - \{[0]\}$ under multiplication
- symmetric-group[214] — the group of bijections of $\{1, \ldots, n\}$, the course's non-abelian example

[210] courses/math1061/subgroups-and-cyclic-groups.pdf
[211] courses/math1061/practice-problems.pdf
[212] courses/math1061/cayley-tables.pdf
[213] courses/math1061/integers-modulo-n.pdf
[214] courses/math1061/symmetric-group.pdf

- subgroups-and-cyclic-groups[215] — subgroups, powers of an element, cyclic subgroups and cyclic groups
- fields[216] — two abelian groups on one set, under + and under ·, joined by the distributive laws
- composition-of-functions[217] — the operation of S_n and of the group of functions $ax + b$
- quantified-statements[218] — the two orders of quantifiers in the identity and inverse properties
- proof-techniques[219] — direct proof and counterexample, the methods the checks use
- 2026-09-24-definitions-and-examples-of-groups[220] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[221] — Lecture 27
- practice-problems[222] — §33, with full worked solutions · practice-problems[223] — §34

Hasse Diagrams

The arrow diagram of a partial order carries a lot of arrows that the three properties already guarantee. A Hasse diagram leaves those out and keeps only what cannot be worked out. Partial orders are in partial-order-relations[224], and arrow diagrams in relations-on-sets[225]. First met in 2026-09-22-partial-order-relations[226].

The four steps

A Hasse diagram for a partial order relation is obtained from its arrow diagram by:-

1. placing the elements so that all the arrows point upwards.
2. delete the loops (the arrows from elements to themselves).
3. delete the arrows which are implied by the transitive property.
4. delete the direction indicators on the arrows.

A Hasse diagram is sufficient to define a partial order relation.

[215] courses/math1061/subgroups-and-cyclic-groups.pdf
[216] courses/math1061/fields.pdf
[217] courses/math1061/composition-of-functions.pdf
[218] courses/math1061/quantified-statements.pdf
[219] courses/math1061/proof-techniques.pdf
[220] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[221] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[222] courses/math1061/practice-problems.pdf
[223] courses/math1061/practice-problems.pdf
[224] courses/math1061/partial-order-relations.pdf
[225] courses/math1061/relations-on-sets.pdf
[226] courses/math1061/2026-09-22-partial-order-relations.pdf

The relation has to be a **partial order**. Each step leans on its properties, and that is why nothing is lost:

Step	Why it is safe
1. arrows point up	Needs antisymmetric and transitive together. If arrows led from an element round through others and back to it, transitivity would join two of them both ways, and antisymmetry forbids that. With no such round trips, the elements can be arranged so that every arrow climbs.
2. delete the loops	The relation is reflexive, so every element has a loop. Drawing them says nothing.
3. delete the implied arrows	The relation is transitive, so an arrow $x \to z$ that follows from $x \to y$ and $y \to z$ can be put back.
4. delete the arrowheads	After step 1, every line points up.

A six-element example is worked step by step in 2026-09-22-partial-order-relations[227].

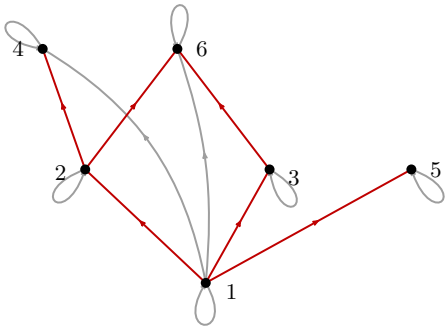
Step 3 in practice: delete $x \to z$ whenever there is some other element y with $x \to y$ and $y \to z$. What survives are the arrows from an element to one **directly** above it, with nothing in between.

Worked: divides on $\{1, 2, \ldots, 6\}$

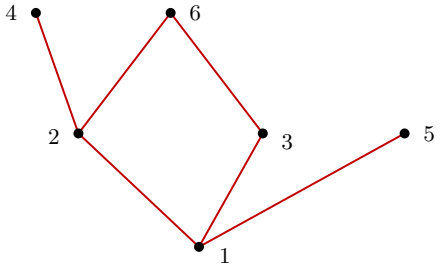
The arrow diagram of $x \mid y$ on $\{1, \ldots, 6\}$ is drawn in reflexive-symmetric-and-transitive-relations[228], already arranged with every arrow pointing up. It has 14 arrows.

1. **Arrows point up.** Put 1 at the bottom, since it divides everything. Above it go 2, 3 and 5, and above them 4 and 6.
2. **Delete the loops.** Six go, leaving eight: $1 \to 2$, $1 \to 3$, $1 \to 5$, $2 \to 4$, $2 \to 6$, $3 \to 6$, $1 \to 4$, $1 \to 6$.
3. **Delete the implied arrows.** $1 \to 4$ follows from $1 \to 2 \to 4$, and $1 \to 6$ follows from $1 \to 2 \to 6$ (and from $1 \to 3 \to 6$). Two go, leaving six.
4. **Delete the arrowheads.**

[227] courses/math1061/2026-09-22-partial-order-relations.pdf
[228] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf



arrow diagram: 14 arrows
6 loops and 2 implied arrows in grey



Hasse diagram: 6 lines

Figure 36: The relation $x \mid y$ on $1, \ldots, 6$, as an arrow diagram and as a Hasse diagram. Left: all 14 arrows. The 8 that the steps delete are grey: the 6 loops, and the arrows $1 \to 4$ and $1 \to 6$, which the transitive property implies. Right: the 6 that remain, without arrowheads. A number divides another exactly when a path leads from it up to the other, so $1 \mid 6$ still shows, by way of 2 or 3. 5 is joined only to 1, since it divides none of the others and only 1 divides it.

Reading a Hasse diagram

A Hasse diagram is *sufficient to define* the relation: nothing was lost in drawing it. To read the relation back, undo the steps:

$x \, R \, y$ exactly when $x = y$, or there is a path from x to y that goes upward all the way.

- $x = y$ restores the loops (step 2).
- A path of one line is an arrow that was kept.
- A path of two or more lines restores an implied arrow (step 3).
- "Upward" restores the direction (step 4).

For the six-element example the count comes back as 6 loops, 6 kept arrows and 6 implied arrows, 18 in all.

The same rule reads off the other notions of partial-order-relations[229]:

- **Comparable**: two different elements are comparable exactly when an upward path joins them, starting from either one.
- **Non-comparable**: no upward path either way. Two elements drawn at the same height are never comparable, because every line climbs.

[229] courses/math1061/partial-order-relations.pdf

- **Total order**: the whole diagram is a single column, one element above the other.

A path that goes up and then comes down does not count. In the diagram of $\subseteq$ on $\mathcal{P}(\{1,2,3\})$ you can get from $\{1\}$ to $\{2,3\}$ along lines, but only by going down at some point. $\{1\} \not\subseteq \{2,3\}$, and the two are not comparable.

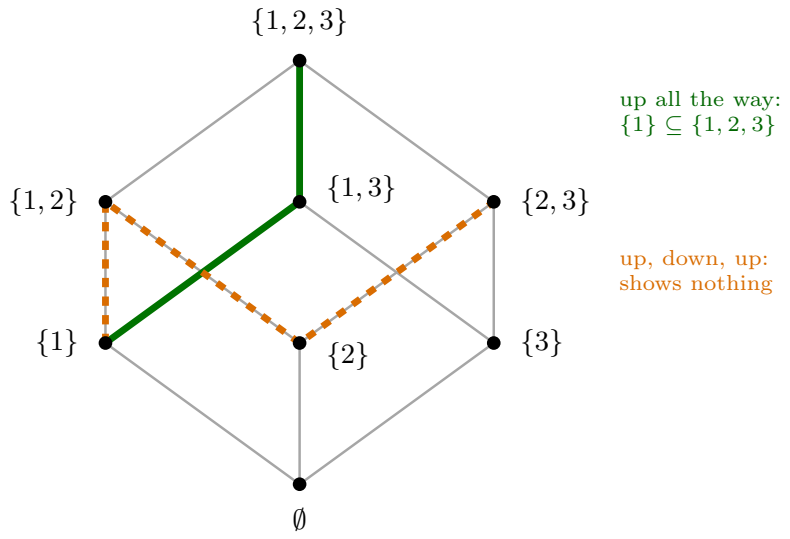


Figure 37: Reading the Hasse diagram of $\subseteq$ on $\mathcal{P}(1,2,3)$. The green path climbs at every step, from 1 through $1,3$ to $1,2,3$, so $1 \subseteq 1,2,3$ and the two sets are comparable. The dashed orange path also joins two sets, 1 and $2,3$, but it goes up, then down, then up. It does not show a relation. No path from 1 climbs all the way to $2,3$, and none climbs from $2,3$ to 1, so those two sets are not comparable.

The diagrams in the course so far

Partial order	Its Hasse diagram	Where
six elements a to f	a column a, b, c, d, e with f joined to a and e	2026-09-22-partial-order-relations[230]
$\subseteq$ on $\mathcal{P}(\{1,2,3\})$	a cube standing on a corner, 12 lines	2026-09-22-partial-order-relations[231]
divides on $\{1, \ldots, 6\}$	6 lines, above	above
divides on $\{1,2,4,8,16\}$	a single column	partial-order-relations[232]

[230] courses/math1061/2026-09-22-partial-order-relations.pdf
[231] courses/math1061/2026-09-22-partial-order-relations.pdf
[232] courses/math1061/partial-order-relations.pdf

In the power-set diagram each line adds exactly one element to a set. In the divides diagram above each line multiplies by a prime: $1 \to 2$, $1 \to 3$, $1 \to 5$, $2 \to 4$, $2 \to 6$, $3 \to 6$. In both cases a line is a single smallest step up.

Common mistakes

- **Keeping an implied line.** If x is joined up to y and y up to z, there is no line from x to z. A triangle in a Hasse diagram is always wrong.
- **A horizontal line.** Every line has to climb, or the deleted arrowhead cannot be recovered.
- **Putting the larger element lower.** The relation reads upward. For divides, 1 is at the bottom. For $\subseteq$, $\emptyset$ is.
- **Reading only the lines as the relation.** The lines are the kept arrows. The relation also contains every loop and every implied arrow.
- **Drawing one for a relation that is not a partial order.** If two different elements are related both ways, step 1 cannot be done.
- **Treating any path as a comparison.** The path must go upward at every step.

See also

- partial-order-relations[233] — partial and total orders, and comparable elements
- antisymmetric-relations[234] — the property that lets the arrows all point one way
- relations-on-sets[235] — the full arrow diagram a Hasse diagram is cut down from
- reflexive-symmetric-and-transitive-relations[236] — loops and short cuts, the arrows steps 2 and 3 delete
- 2026-09-22-partial-order-relations[237] — Lecture 25
- practice-problems[238] — §32, with full worked solutions

The Integers Modulo n

$\mathbb{Z}_n$ is the set of equivalence classes of congruence mod n. It is a number system with exactly n elements, in which addition and multiplication are done on classes. Congruence itself is in modular-arithmetic[239], and equivalence classes in equivalence-classes-and-partitions[240]. Under addition $\mathbb{Z}_n$ is one of the course's standard [groups], and when n is prime it is a field, with

[233] courses/math1061/partial-order-relations.pdf
[234] courses/math1061/antisymmetric-relations.pdf
[235] courses/math1061/relations-on-sets.pdf
[236] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[237] courses/math1061/2026-09-22-partial-order-relations.pdf
[238] courses/math1061/practice-problems.pdf
[239] courses/math1061/modular-arithmetic.pdf
[240] courses/math1061/equivalence-classes-and-partitions.pdf

division by every non-zero class (fields[241]). First met in 2026-09-24-definitions-and-examples-of-groups[242].

The set $\mathbb{Z}_n$

Fix $n \in \mathbb{Z}^+$. Congruence mod n is an equivalence relation on $\mathbb{Z}$,

$$m \; R \; k \iff m \equiv k \pmod{n} \iff n \mid (m-k),$$

and its classes partition $\mathbb{Z}$. $\mathbb{Z}_n$ is the set of those classes:

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}.$$

For $n = 10$:

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

$$[0] = \{\dots, -30, -20, -10, 0, 10, 20, 30, \dots\}, \qquad [1] = \{\dots, -29, -19, -9, 1, 11, 21, 31, \dots\}$$

- $\mathbb{Z}_n$ **has exactly** n **elements.** Every integer leaves exactly one of the remainders $0, 1, \dots, n-1$ on division by n (modular-arithmetic[243]), so every integer is in exactly one of the n classes.
- **Each element is an infinite set of integers.** $[1]$ is not the number 1. It is the set of all integers congruent to 1.
- **Each class has many names.** $[0] = [10] = [30]$ and $[1] = [21] = [-9]$. In general $[a] = [b]$ exactly when $a \equiv b \pmod{n}$ (equivalence-classes-and-partitions[244]).

  We usually use $[0], [1], \dots, [n-1]$ as representatives for the equivalence classes of $\mathbb{Z}_n$.

Adding and multiplying classes

Define binary operations $+$ (plus/addition) and $\cdot$ (times/multiplication) on $\mathbb{Z}_n$ as follows. For all $[a], [b] \in \mathbb{Z}_n$,

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

To combine two classes, combine a representative of each in the ordinary way and take the class of the result. In $\mathbb{Z}_{10}$: $[8] + [9] = [17] = [7]$ and $[8] \cdot [9] = [72] = [2]$.

[241] courses/math1061/fields.pdf
[242] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[243] courses/math1061/modular-arithmetic.pdf
[244] courses/math1061/equivalence-classes-and-partitions.pdf

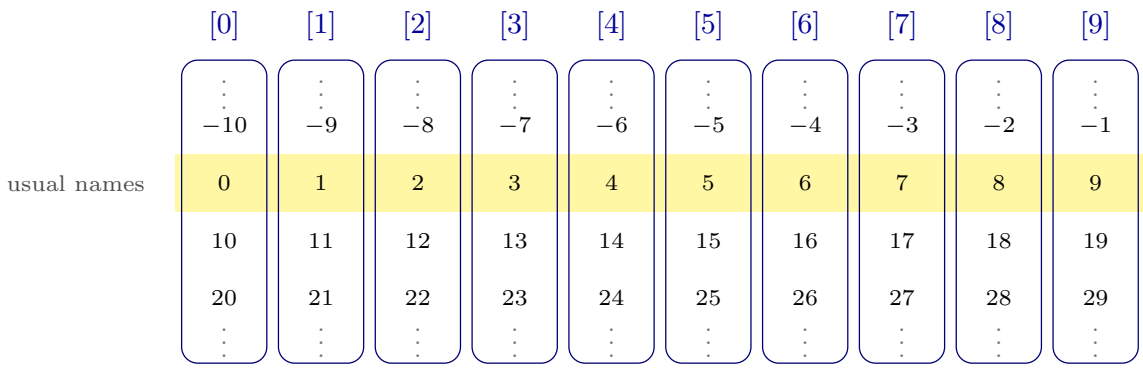


Figure 38: The integers from −10 to 29 written in rows of ten. Each column is one element of $\mathbb{Z}_{10}$: going down a column adds 10, so everything in a column is congruent mod 10. The whole of $\mathbb{Z}$ is sorted into these ten columns, and $\mathbb{Z}_{10}$ is the set of the ten columns. The shaded row holds the usual representatives, 0 to 9. Any other number in a column names the same class, so $[21] = [1]$ and $[-1] = [9]$.

Any representative can be used

> when doing arithmetic in $\mathbb{Z}_n$, any representative of the equivalence classes can be used.

The definition $[a] + [b] = [a + b]$ computes with the particular names a and b, and each class has infinitely many names. The boxed sentence says the result does not depend on which names are used.

The reason is the lemma of modular-arithmetic[245]: if $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$a + b \equiv a' + b' \pmod{n} \qquad \text{and} \qquad ab \equiv a'b' \pmod{n}.$$

In the language of classes, if $[a] = [a']$ and $[b] = [b']$ then $[a + b] = [a' + b']$ and $[ab] = [a'b']$.

Choosing a convenient representative

Since any representative will do, pick the one that makes the arithmetic easy, and reduce at any stage. For example:

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

[245] courses/math1061/modular-arithmetic.pdf

+	−1	9	19
−2	−3	7	17
8	7	17	27
18	17	27	37

every sum is $\equiv 7 \pmod{10}$
$[8] + [9] = [7]$

·	−1	9	19
−2	2	−18	−38
8	−8	72	152
18	−18	162	342

every product is $\equiv 2 \pmod{10}$
$[8] \cdot [9] = [2]$

Figure 39: $[8] + [9]$ and $[8] \cdot [9]$ in $\mathbb{Z}_{10}$, computed with three different representatives of each class: -2, 8 and 18 for $[8]$ down the side, and -1, 9 and 19 for $[9]$ across the top. The sums are not all the same integer, but every one of them is congruent to 7. The products are not all the same integer, but every one is congruent to 2. Whichever representatives are used, $[8] + [9] = [7]$ and $[8] \cdot [9] = [2]$.

$[9]$ became $[-1]$ and $[7]$ became $[-3]$. A representative just below a multiple of n is often better written as a small negative number. Without the swap the same calculation is $[17] \cdot [13] = [221] = [1]$.

$(\mathbb{Z}_n, +)$ is a group

For every $n \in \mathbb{Z}^+$, $(\mathbb{Z}_n, +)$ is a group. The check of the four properties (groups[246]):

- **Closure.** $[a] + [b] = [a + b]$, which is a class in $\mathbb{Z}_n$.
- **Associativity.** $([a] + [b]) + [c] = [(a + b) + c] = [a + (b + c)] = [a] + ([b] + [c])$. It is inherited from addition of integers.
- **Identity.** $[0]$, since $[0] + [a] = [a] + [0] = [a]$.
- **Inverses.** $[a]^{-1} = [-a]$, since $[a] + [-a] = [-a] + [a] = [0]$. With the usual names, $[-a] = [n - a]$.

It is abelian, because $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.

For $n = 3$, one of the eight candidates of groups[247]:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

[246] courses/math1061/groups.pdf
[247] courses/math1061/groups.pdf

Here the group inverse of [1] is [2], because $[1]+[2]=[0]$. In an additive group the "inverse" is the negative.

Multiplication: $\mathbb{Z}_n - \{[0]\}$

Multiplication of classes is closed, associative and commutative on $\mathbb{Z}_n$, with identity [1]. But $(\mathbb{Z}_n, \cdot)$ is not a group when $n > 1$: $[0] \cdot [a] = [0]$ for every $[a]$, so [0] has no inverse. This is the same obstacle as 0 in $(\mathbb{R}, \cdot)$, and the same repair is tried, removing it.

	Group under multiplication?	Worked in
$\mathbb{Z}_5 - \{[0]\}$	**yes**	2026-09-24-definitions-and-examples-of-groups[248]; table in practice-problems[249], Q4
$\mathbb{Z}_7 - \{[0]\}$	**yes**	2026-09-24-definitions-and-examples-of-groups[250]
$\mathbb{Z}_9 - \{[0]\}$	**no**: not closed, $[3] \cdot [3] = [9] = [0]$	the same practice set, Q1
$\{[1],[2],[4],[5],[7],[8]\}$ in $\mathbb{Z}_9$	**yes**	the same practice set, Q3
$\mathbb{Z}_4 - \{[0]\}$	**no**: not closed, $[2] \cdot [2] = [4] = [0]$	2026-10-08-definitions-and-examples-of-fields[251]
$\mathbb{Z}_{15} - \{[0]\}$	**no**: not closed, $[3] \cdot [5] = [15] = [0]$	2026-10-08-definitions-and-examples-of-fields[252]

For $n = 9$, removing [0] is not enough. [3] and [6] multiply into [0], and removing those as well leaves a group.

The rule: $\mathbb{Z}_n - \{[0]\}$ is a group under multiplication exactly when n is prime. When $n = rs$ is composite, with $1 < r, s < n$, the non-zero classes $[r]$ and $[s]$ have $[r] \cdot [s] = [n] = [0]$, and closure fails, as for $9 = 3 \cdot 3$, $4 = 2 \cdot 2$ and $15 = 3 \cdot 5$. When n is prime, no product of non-zero classes is [0] and every non-zero class has an inverse. Why is in fields[253].

$\mathbb{Z}_p$ is a field

$(\mathbb{Z}_p, +, \cdot)$ is a field when p is prime. All three conditions of fields[254] hold:

[248] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[249] courses/math1061/practice-problems.pdf
[250] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[251] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[252] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[253] courses/math1061/fields.pdf
[254] courses/math1061/fields.pdf

1. $(\mathbb{Z}_p, +)$ is an abelian group, as above.
2. $(\mathbb{Z}_p - \{[0]\}, \cdot)$ is an abelian group, by the rule just stated.
3. The distributive laws are inherited from the integers: $[a] \cdot ([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$.

So in $\mathbb{Z}_p$ every class can be subtracted and every non-zero class divided by, and every equation $[a]x + [b] = [c]$ with $[a] \neq [0]$ has exactly one solution (fields[255]). For composite n, $\mathbb{Z}_n$ is not a field. $\mathbb{Z}_7$ is, and $\mathbb{Z}_4$ and $\mathbb{Z}_{15}$ are not (2026-10-08-definitions-and-examples-of-fields[256]).

Finding a multiplicative inverse

The inverse of $[a]$ is the class $[b]$ with $ab \equiv 1 \pmod{n}$. Read it from the Cayley table, as in 2026-09-24-definitions-and-examples-of-groups[257], or search: in $\mathbb{Z}_7$, $[3] \cdot [5] = [15] = [1]$, so $[3]^{-1} = [5]$. This is the relation $xy \equiv 1 \pmod{7}$, whose arrow diagram is in 2026-09-17-relations-reflexivity-symmetry-transitivity[258]: each non-zero number is joined to its inverse.

When there is no table, there are three ways in:

- **List the multiples.** Write $a, 2a, 3a, \ldots$ mod p, each one the previous plus a, reduced, until 1 appears. For $[10]$ in $\mathbb{Z}_{17}$ the list is $10, 3, 13, 6, 16, 9, 2, 12, 5, 15, 8, 1$, so $10 \cdot 12 \equiv 1$ and $[10]^{-1} = [12]$. The search is drawn in 2026-10-08-definitions-and-examples-of-fields[259]. In $\mathbb{Z}_p$ it always succeeds within $p - 1$ steps, because the multiples of a non-zero class run through every non-zero class.
- **Stop at -1.** If $ab \equiv -1$, then $a \cdot (-b) \equiv 1$, so $[a]^{-1} = [-b]$. In the same list, $10 \cdot 5 = 50 \equiv 16 = -1 \pmod{17}$, so $[10]^{-1} = [-5] = [12]$ after five steps instead of twelve.
- **Quick cases.** $[1]^{-1} = [1]$ and $[p - 1]^{-1} = [p - 1]$, since $(-1)(-1) = 1$. For odd p, $[2]^{-1} = [\frac{p+1}{2}]$, since $2 \cdot \frac{p+1}{2} = p + 1 \equiv 1$. In $\mathbb{Z}_{11}$ that gives $[2]^{-1} = [6]$.

The inverses in three small fields, each pair being inverses of each other:

p	Own inverse	Pairs
5	[1], [4]	[2] ↔ [3]
7	[1], [6]	[2] ↔ [4], [3] ↔ [5]
11	[1], [10]	[2] ↔ [6], [3] ↔ [4], [5] ↔ [9], [7] ↔ [8]

In a composite $\mathbb{Z}_n$ the search can fail. The multiples of $[2]$ in $\mathbb{Z}_6$ are $[2], [4], [0], [2], \ldots$, and $[1]$ never appears, so $[2]$ has no inverse there.

[255] courses/math1061/fields.pdf
[256] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[257] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[258] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf
[259] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

Notation

- **Three ways to say one thing.** $n \mid (a-b)$, $a \equiv b \pmod{n}$, and $[a] = [b]$ in $\mathbb{Z}_n$ are the same statement. The first is about divisibility, the second about integers, the third about classes.
- **$=$ for classes, $\equiv$ for integers.** $[7] = [0]$ in $\mathbb{Z}_7$ is true. $7 = 0$ is false. $7 \equiv 0 \pmod{7}$ is true.
- **Brackets are often dropped.** The practice problems write $\mathbb{Z}_9 - \{0\} = \{1, 2, \ldots, 8\}$ and "$2 \cdot 5 = 10 \equiv 1 \pmod{9}$" for what is written here as $\mathbb{Z}_9 - \{[0]\}$ and $[2] \cdot [5] = [10] = [1]$. It is the same arithmetic.
- **The $-$ in $\mathbb{Z}_7 - \{[0]\}$ is set difference** (sets-and-set-notation[260]): the set $\mathbb{Z}_7$ with the one element $[0]$ removed.
- mod **again.** The remainder $a \bmod n$ is the usual representative of $[a]$ (modular-arithmetic[261]).

Common mistakes

- **Treating $[a]$ as the integer a.** $[9] = [-1]$ in $\mathbb{Z}_{10}$, but $9 \neq -1$.
- **Thinking $\mathbb{Z}_n$ is infinite.** It has n elements. Each element is an infinite set.
- **Using the wrong inverse.** In $(\mathbb{Z}_7, +)$ the inverse of $[3]$ is $[4]$. In $(\mathbb{Z}_7 - \{[0]\}, \cdot)$ it is $[5]$. Look at the operation first.
- **Dividing.** There is no $[\frac{1}{2}]$. An "inverse of $[2]$" under multiplication means a class $[b]$ with $[2][b] = [1]$, and it may not exist. In $\mathbb{Z}_p$ it always does: in $\mathbb{Z}_{11}$ it is $[6]$, so "dividing by 2" there means multiplying by $[6]$.
- **Mixing up the two inverses.** To undo $+[3]$ in $\mathbb{Z}_{11}$, add $-[3] = [8]$. To undo $[2]\cdot$, multiply by $[2]^{-1} = [6]$.
- **Not checking closure after removing elements.** $\mathbb{Z}_9 - \{[0]\}$ is the example.

See also

- modular-arithmetic[262] — congruence, remainders, and the lemma that makes class arithmetic work
- equivalence-classes-and-partitions[263] — classes and representatives in general
- [groups] — the definition $\mathbb{Z}_n$ is checked against
- fields[264] — why $\mathbb{Z}_n$ is a field exactly when n is prime, and solving equations in $\mathbb{Z}_p$

[260] courses/math1061/sets-and-set-notation.pdf
[261] courses/math1061/modular-arithmetic.pdf
[262] courses/math1061/modular-arithmetic.pdf
[263] courses/math1061/equivalence-classes-and-partitions.pdf
[264] courses/math1061/fields.pdf

- subgroups-and-cyclic-groups[265] — cyclic subgroups and cyclic groups; $(\mathbb{Z}_n, +)$ is cyclic, generated by [1]
- cayley-tables[266] — the tables for $\mathbb{Z}_7 - \{[0]\}$ and $\mathbb{Z}_5 - \{[0]\}$ and how to read them
- 2026-09-24-definitions-and-examples-of-groups[267] — Lecture 26 · 2026-09-21-equivalence-relations[268] — Lecture 24, where the classes of congruence mod 3 are drawn
- 2026-10-06-elementary-properties-of-groups[269] — Lecture 27, where powers and cyclic subgroups are worked in $\mathbb{Z}_7 - \{[0]\}$, $\mathbb{Z}_{11} - \{[0]\}$ and $\mathbb{Z}_8$
- 2026-10-08-definitions-and-examples-of-fields[270] — Lecture 28, where $\mathbb{Z}_4$, $\mathbb{Z}_7$ and $\mathbb{Z}_{15}$ are tested and equations are solved in $\mathbb{Z}_{11}$ and $\mathbb{Z}_{17}$
- practice-problems[271] — §33, with full worked solutions
- practice-problems[272] — §36, equations in $\mathbb{Z}_5$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$ and $\mathbb{Z}_{19}$

Modular Arithmetic, Floor & the Quotient-Remainder Theorem

Floor and ceiling

For a real number x:

- $\lfloor x \rfloor$ — the **floor**: move **left** on the number line to the nearest integer.
- $\lceil x \rceil$ — the **ceiling**: move **right** on the number line to the nearest integer.

So $\lfloor -3.2 \rfloor = -4$ and $\lceil -3.2 \rceil = -3$; $\lfloor 3.2 \rfloor = 3$ and $\lceil 3.2 \rceil = 4$. **Negative numbers are where this goes wrong most often** — floor of -3.2 is -4, not -3.

To use floor or ceiling in a proof, it is usually easiest to rewrite the expression as **an integer plus an amount between 0 and 1**. For instance, in proving "if n is an odd integer then $\lceil \frac{n}{2} \rceil = \lfloor \frac{n}{2} \rfloor + 1$", write

$$\frac{n}{2} = \frac{2k+1}{2} = k + \frac{1}{2}$$

for some integer k; then $k + \frac{1}{2}$ sits strictly between k and $k+1$, so the floor is k and the ceiling is $k+1$. The same move handles things like $\lfloor (p^3 + 4p^2 + 5) + \frac{1}{4} \rfloor$ where $p \in \mathbb{Z}$.

Two ways to compute $\lfloor \frac{-32}{5} \rfloor$:

- *Fraction approach*: $\lfloor \frac{-32}{5} \rfloor = \lfloor \frac{-30}{5} - \frac{2}{5} \rfloor = \lfloor -6 - \frac{2}{5} \rfloor = -7$ (something smaller than -6).

[265] courses/math1061/subgroups-and-cyclic-groups.pdf
[266] courses/math1061/cayley-tables.pdf
[267] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[268] courses/math1061/2026-09-21-equivalence-relations.pdf
[269] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[270] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[271] courses/math1061/practice-problems.pdf
[272] courses/math1061/practice-problems.pdf

- *Decimal approach*: $\lfloor -6.4 \rfloor = \lfloor -6 - 0.4 \rfloor = -7$.

And $\lceil \frac{-32}{5} \rceil = -6$.

$\forall x \in \mathbb{R}, \lfloor x^2 \rfloor = \lfloor x \rfloor^2$ **is false** — take $x = \frac{3}{2}$: $\lfloor \frac{9}{4} \rfloor = 2$ but $\lfloor \frac{3}{2} \rfloor^2 = 1^2 = 1$.

The quotient-remainder theorem

Given any integer n and positive integer d, there exist **unique** integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d$$

q is the **quotient** ($n \operatorname{div} d$) and r is the **remainder** ($n \bmod d$). Explicitly:

$$q = \left\lfloor \frac{n}{d} \right\rfloor \qquad r = n - d \left\lfloor \frac{n}{d} \right\rfloor$$

With $d = 6$:

n	$n = dq + r$	q	r
53	$6 \cdot 8 + 5$	8	5
20	$6 \cdot 3 + 2$	3	2
-19	$6 \cdot (-4) + 5$	-4	5

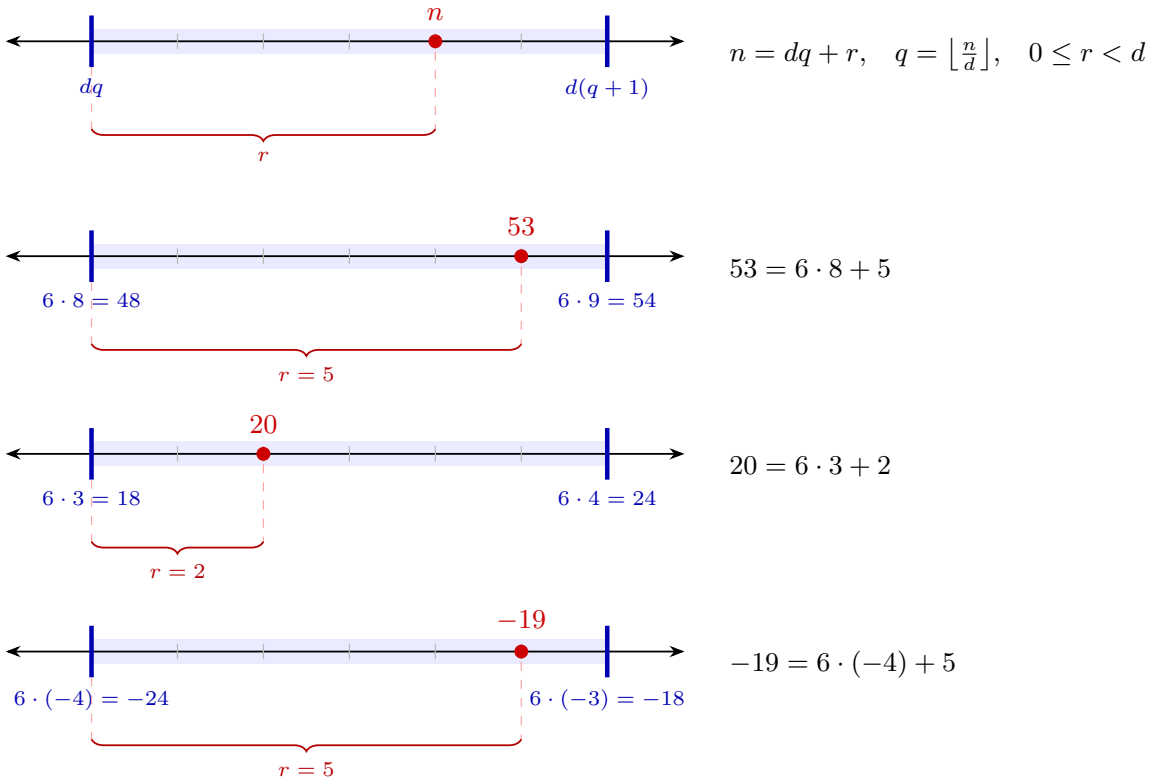
Negative n is the case to watch: the remainder is still required to be non-negative, so $-19 \bmod 6 = 5$, not -1. Likewise $-95 = 11(-9) + 4$, so $-95 \operatorname{div} 11 = -9$ and $-95 \bmod 11 = 4$. And $58 = 11 \cdot 5 + 3$, so $58 \operatorname{div} 11 = 5$, $58 \bmod 11 = 3$.

mod versus $\equiv$ — take care with notation

These are different statements.

- $n \bmod d = r$ — an *equality between numbers*: the remainder when n is divided by d is r, with $0 \leq r < d$.
- $m \equiv n \pmod{d}$ — a *relation between m and n*: they leave the same remainder when divided by d.

Example: $5 \bmod 4 = 1$ and $9 \bmod 4 = 1$, so $9 \equiv 5 \pmod 4$ — but $9 \bmod 4 \neq 5$.



The shaded band is the half-open block $[\,dq,\ d(q+1)\,)$ that n lands in. The quotient q names the multiple of d at or *below* n, so the remainder r is always measured rightwards — which is why -19 has remainder 5 and not -1.

Figure 40: Why the remainder is never negative: the general case and the three $d = 6$ examples on the number line. Each shaded band is one block $[dq, d(q+1))$ of width d; the quotient names the multiple of d at or below n, so r is always the rightward gap from that multiple, and -19 therefore has remainder 5 rather than -1.

Two equivalent definitions of congruence

For $m, n, d \in \mathbb{Z}$ with $d > 0$:

- **Definition 1**: $m \equiv n \pmod{d}$ iff m and n have the same remainder under the quotient-remainder theorem.
- **Definition 2**: $m \equiv n \pmod{d}$ iff $d \mid (m - n)$.

Definition 2 is usually the faster one to check, and the one to reach for in proofs (see divisibility-and-factorisation[273]).

Worked both ways — is $-50 \equiv 22 \pmod{8}$?

- *Definition 1*: $-50 = -56 + 6 = 8(-7) + 6$, so $-50 \bmod 8 = 6$; and $22 = 16 + 6$, so $22 \bmod 8 = 6$. Same remainder, so yes.
- *Definition 2*: $22 - (-50) = 72 = 8 \cdot 9$, so $8 \mid (22 - (-50))$, so yes.

Similarly $53 \equiv -19 \pmod{6}$ (both leave remainder 5; and $53 - (-19) = 72$ is divisible by 6), while $53 \not\equiv 20 \pmod{6}$.

Arithmetic with congruences

Lemma: if $a \equiv b \pmod{d}$ and $m \equiv n \pmod{d}$, then

$$a + m \equiv b + n \pmod{d} \qquad \text{and} \qquad am \equiv bn \pmod{d}$$

That is, you may substitute any number for a congruent one *before* adding or multiplying — which is what makes modular arithmetic cheap.

For example, $8 \equiv 2 \pmod{3}$ and $46 \equiv 1 \pmod{3}$, so $8 \cdot 46 \equiv 2 \cdot 1 \equiv 2 \pmod{3}$ and $8 + 46 \equiv 2 + 1 \equiv 0 \pmod{3}$.

Worked: suppose $x \bmod 6 = 4$ and $y \bmod 6 = 3$.

- $(x + y) \bmod 6$: $x + y \equiv 4 + 3 \equiv 7 \equiv 1 \pmod{6}$, so the answer is 1.
- $(5x^2 + 4y) \bmod 6$: $5x^2 + 4y \equiv 5(4)^2 + 4(3) \equiv 5(16) + 12 \equiv 5(4) \equiv 20 \equiv 2 \pmod{6}$ — applying the lemma at each step.

Worked: if $m \bmod 6 = 4$, what is $35m \bmod 6$? Since $35 \bmod 6 = 5$, $35m \equiv 5 \cdot 4 \equiv 20 \equiv 2 \pmod{6}$. And $3m^2 + 2m + 1 \equiv 3(4)^2 + 2(4) + 1 \equiv 12(4) + 8 + 1 \equiv 8 + 1 \equiv 3 \pmod{6}$ — $3 \cdot 4^2$ is $12 \cdot 4$, and that term drops out whole, since $6 \mid 12$.

Worked: an integer n leaves remainder 4 on division by 7 — what is the remainder of $3n$? Write $n = 7k + 4$; then $3n = 21k + 12 = 7(3k + 1) + 5$, so the remainder is 5. (The course's

[273] courses/math1061/divisibility-and-factorisation.pdf

solutions PDF has this step as $7(3k)+5$, which is $21k+5$, not $21k+12$; the quotient is $3k+1$. The answer of 5 is unaffected — see practice-problems[274].)

Worked: m leaves remainder 9 on division by 11 — what remainder does $4m$ leave on division by **22**? Write $m = 11k+9$; then $4m = 44k+36 = 22(2k+1)+14$, so the remainder is 14. (Note the modulus changed, so you cannot just reduce mod 11.)

Divisibility tests

Modular arithmetic explains the familiar tests. **A positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3**, because $10 \equiv 1 \pmod 3$ and hence $10^k \equiv 1 \pmod 3$ for every $k \in \mathbb{Z}^+$ (apply the multiplication half of the lemma repeatedly: $10^2 \equiv 1$ from $a = m = 10$, $b = n = 1$; then $10^3 \equiv 1$ from $a = 10^2$, $m = 10$; and so on).

$$254 \equiv 2 \cdot 100 + 5 \cdot 10 + 4 \cdot 1 \equiv 2 + 5 + 4 \equiv 11 \equiv 2 \pmod 3$$

so 254 is not divisible by 3 and leaves remainder 2 (checking: $254 = 3 \cdot 84 + 2$). Whereas

$$3252 \equiv 3 + 2 + 5 + 2 \equiv 12 \equiv 0 \pmod 3$$

so $3 \mid 3252$.

Worked proofs

For any odd integer n, $n^2 \bmod 4 = 1$.

> Suppose n is odd, so $n = 2k+1$ for some $k \in \mathbb{Z}$. Then
>
> $$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k) + 1.$$
>
> Since $k^2 + k \in \mathbb{Z}$ and $0 \le 1 < 4$, the quotient-remainder theorem gives $n^2 \bmod 4 = 1$. □

Hence for any odd integer n, $\left\lfloor \frac{n^2}{4} \right\rfloor = \frac{n^2-1}{4}$. Two routes:

- *Method 1 — expand both sides.* With $n = 2k+1$: LHS $= \left\lfloor \frac{4k^2+4k+1}{4} \right\rfloor = \left\lfloor (k^2+k) + \frac{1}{4} \right\rfloor = k^2 + k$. RHS $= \frac{(2k+1)^2-1}{4} = \frac{4k^2+4k}{4} = k^2 + k$. Equal.
- *Method 2 — use $r = n - d\lfloor \frac{n}{d} \rfloor$.* With number n^2, divisor 4, remainder 1: $1 = n^2 - 4\lfloor \frac{n^2}{4} \rfloor$, so $4\lfloor \frac{n^2}{4} \rfloor = n^2 - 1$ and $\lfloor \frac{n^2}{4} \rfloor = \frac{n^2-1}{4}$.

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

For all odd integers n, $\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)$ — true, since with $n = 2k+1$ the right-hand side is $\frac{2k}{2} \cdot \frac{2k+2}{2} = k(k+1)$, matching the $k^2 + k$ above.

If y is any integer, then y^2 divided by 5 leaves remainder 0, 1 or 4 — never 2 or 3.

> Fix $y \in \mathbb{Z}$. By the quotient-remainder theorem, $y = 5m + r$ for some $m \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3, 4\}$. Then
>
> $$y^2 = 25m^2 + 10mr + r^2 \equiv r^2 \pmod 5.$$
>
> Checking each case: $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9 \equiv 4$, $4^2 \equiv 16 \equiv 1 \pmod 5$. So $y^2 \equiv 0, 1$ or $4 \pmod 5$. $\square$

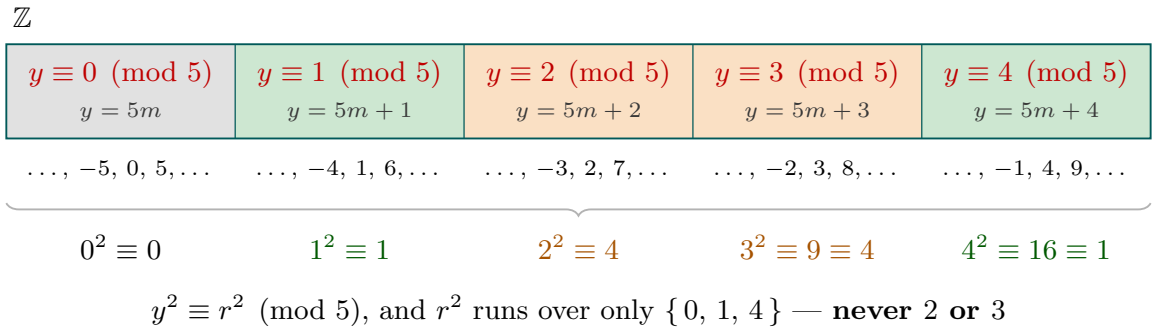


Figure 41: The case split the proof above runs on: $\mathbb{Z}$ cut into the five residue classes mod 5. The tints group the classes by the remainder their square leaves, which is what makes 2 and 3 unreachable.

This "split into cases by remainder" move is the standard way to prove something about *every* integer using modular arithmetic.

See also

- divisibility-and-factorisation[275] · gcd-lcm-and-euclidean-algorithm[276] · proof-techniques[277]
- sets-and-set-notation[278] — congruence classes as sets, and the partitions of $\mathbb{Z}$ they give

[275] courses/math1061/divisibility-and-factorisation.pdf
[276] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[277] courses/math1061/proof-techniques.pdf
[278] courses/math1061/sets-and-set-notation.pdf

- equivalence-relations[279] · integers-modulo-n[280] — congruence as an equivalence relation, and its classes as the number system $\mathbb{Z}_n$
- pigeonhole-principle[281] — the n remainders as pigeonholes: among any $n+1$ integers, two differ by a multiple of n
- practice-problems[282] — §14 Modular Arithmetic, with full worked solutions

One-to-One and Onto Functions

The two properties a function $f : X \to Y$ can have beyond being a function at all — **injective (one-to-one)** and **surjective (onto)** — with the proof templates for showing each and for showing its failure. Together they make a **bijection**, which is what inverse-functions[283] needs. The definition of a function is in functions-on-general-sets[284]; the lecture is 2026-09-07-functions-one-to-one-onto-inverse[285].

The definitions

Let f be a function, $f : X \to Y$.

> **Injective function (one-to-one function):** $\forall x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$.
>
> **Surjective function (onto function):** $\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$.
>
> A function that is both one-to-one and onto is a **bijection**.

In words: **one-to-one** means no two inputs share an output — different inputs, different outputs. **Onto** means every element of the co-domain is hit — the range is the whole of Y. Each name has a Latin and an English form, used interchangeably: *injective / one-to-one*, *surjective / onto*, *bijective / one-to-one correspondence*.

The two are about opposite ends of the arrows. One-to-one is a condition on the **domain side**: arrows never merge. Onto is a condition on the **co-domain side**: nothing is left unreached. They are independent, and all four combinations occur:

For finite sets the picture gives a counting fact for free: one-to-one forces $|X| \leq |Y|$, onto forces $|X| \geq |Y|$, and a bijection forces $|X| = |Y|$. That is the beginning of the next topic,

[279] courses/math1061/equivalence-relations.pdf
[280] courses/math1061/integers-modulo-n.pdf
[281] courses/math1061/pigeonhole-principle.pdf
[282] courses/math1061/practice-problems.pdf
[283] courses/math1061/inverse-functions.pdf
[284] courses/math1061/functions-on-general-sets.pdf
[285] courses/math1061/2026-09-07-functions-one-to-one-onto-inverse.pdf

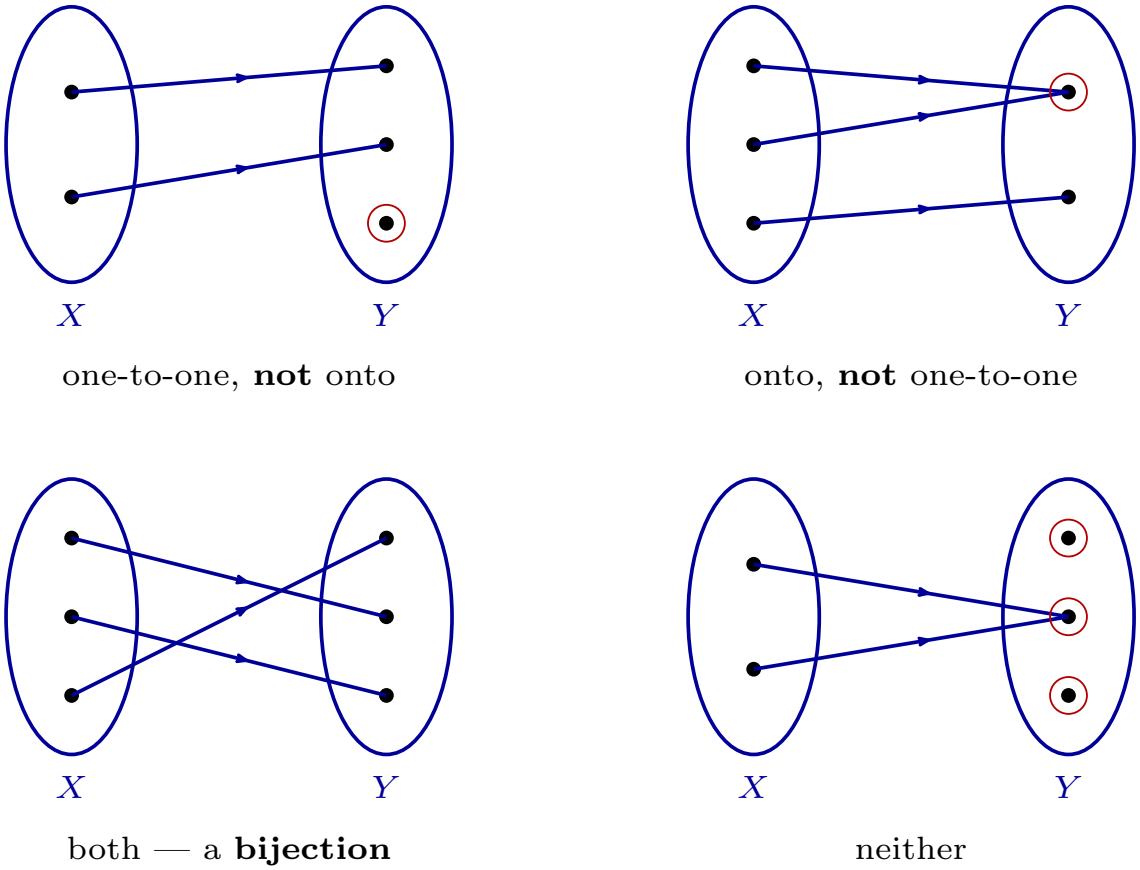


Figure 42: The four combinations, on the smallest sets that show them. Top left: one-to-one but not onto — arrows never merge, but the third dot of Y is missed. Top right: onto but not one-to-one — everything in Y is hit, but two arrows merge. Bottom left: both, a bijection — a perfect pairing. Bottom right: neither. A red ring marks the offending element of Y in each failing panel — a target that two arrows share, or a dot no arrow reaches; in the *neither* panel it marks one of each kind.

cardinality[286], where the same three facts become the definitions of $\leq$, $\geq$ and $=$ for sets of any size.

On the real line

The graph versions of the two tests:

	Test on the graph	Example
one-to-one	no horizontal line meets the graph twice	2^x passes; $x^3 - x$ fails, x^2 fails
onto $\mathbb{R}$	every horizontal line meets the graph at least once	$x^3 - x$ passes; 2^x fails (never ≤ 0), x^2 fails

The *vertical* line test decides whether a curve is a function at all (functions-on-general-sets[287]); the *horizontal* line test decides one-to-one.

Changing the co-domain

Onto depends on the **declared** co-domain, so it can be switched on by declaring a smaller one:

$$f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2 \text{ is not onto;} \qquad g : \mathbb{R} \to \mathbb{R}^{\geq 0},\ g(x) = x^2 \text{ is onto.}$$

Same pairs, different function, because Y is part of what a function is. Any function becomes onto its own range. One-to-one, by contrast, is a fact about the pairs alone and cannot be adjusted by relabelling the co-domain — though it *can* be switched on by shrinking the domain, which is how $\sqrt{\ }$ gets to be the inverse of x^2 on $\mathbb{R}^{\geq 0}$.

How to prove it

To show $f : X \to Y$ is …	Template
one-to-one	Suppose $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$. … Hence $x_1 = x_2$. $\square$
not one-to-one	Exhibit $x_1, x_2 \in X$ with $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.

[286] courses/math1061/cardinality.pdf
[287] courses/math1061/functions-on-general-sets.pdf

To show $f : X \to Y$ is …	Template
onto	Let $y \in Y$. Take $x = \ldots$ *(in terms of y).* Check $x \in X$. Check $f(x) = y$. $\square$
not onto	Exhibit $y \in Y$ such that $f(x) \neq y$ for all $x \in X$ *(and say why).*

The shape follows the quantifiers (quantified-statements[288]). One-to-one and onto are both **universal** statements, so proving them means starting from an arbitrary element and arguing in general; their negations are **existential**, so disproving means producing one witness. This is the same logic as the element method for sets (proving-set-properties[289]), and the same warning applies: **checking examples proves neither property**, it can only disprove one.

One-to-one: algebra

$$g : \mathbb{Z} \to \mathbb{Z}^{\text{odd}},\ g(x) = 2x + 3.$$

Let $x_1, x_2 \in \mathbb{Z}$ with $g(x_1) = g(x_2)$. Then $2x_1 + 3 = 2x_2 + 3$, so $2x_1 = 2x_2$, so $x_1 = x_2$. $\therefore g$ is one-to-one. $\square$

The proof is "undo the function": peel operations off both sides until the inputs are exposed. Every step must be reversible-in-effect — dividing by 2 is fine; squaring both sides would not be, which is exactly why x^2 is not one-to-one.

Onto: solve backwards, then run forwards

Same g. **Scratch work** (not part of the proof): want x with $2x + 3 = y$, so $x = \frac{y-3}{2}$.

Proof. Let $y \in \mathbb{Z}^{\text{odd}}$. Take $x = \frac{y-3}{2}$. Since y is odd, $y - 3$ is even, so $x \in \mathbb{Z}$. And $g(x) = 2 \cdot \frac{y-3}{2} + 3 = y$. $\therefore g$ is onto. $\square$

Three moves, always in this order: **name** the candidate, **check it is in the domain**, **check it maps to** y. The middle one is where onto proofs go wrong. Here it is the only place the oddness of y is used; drop it and the same lines "prove" that $2x + 3$ is onto all of $\mathbb{Z}$, which is false ($y = 4$ needs $x = \frac{1}{2}$).

[288] courses/math1061/quantified-statements.pdf
[289] courses/math1061/proving-set-properties.pdf

Pairs as inputs

$f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f((x, y)) = (y + 1, 2x)$.

One-to-one. Suppose $f((x_1, y_1)) = f((x_2, y_2))$. Then $(y_1 + 1, 2x_1) = (y_2 + 1, 2x_2)$, so $y_1 + 1 = y_2 + 1$ **and** $2x_1 = 2x_2$; hence $y_1 = y_2$ **and** $x_1 = x_2$, so $(x_1, y_1) = (x_2, y_2)$. □

Onto. Let $(a, b) \in \mathbb{R} \times \mathbb{R}$. Take $\left(\frac{b}{2}, a - 1\right) \in \mathbb{R} \times \mathbb{R}$. Then $f\left(\left(\frac{b}{2}, a - 1\right)\right) = ((a - 1) + 1, 2 \cdot \frac{b}{2}) = (a, b)$. □

Two ordered pairs are equal exactly when both coordinates are, so one equation of pairs is **two** equations of numbers, and both must be carried through. The coordinates also cross over — the output's first entry comes from the input's second — which is why the candidate in the onto proof has b first.

Disproofs

$f : \mathbb{Z} - \{-1, 0, 1\} \to \mathbb{Z}^{>1}$, $f(x) =$ the largest prime divisor of x.

Not one-to-one: $f(10) = 5 = f(15)$ and $10 \neq 15$. Not onto: $4 \in \mathbb{Z}^{>1}$, but 4 is not prime, so no x has $f(x) = 4$ — the range of f is the set of primes, a proper subset of $\mathbb{Z}^{>1}$. Both are one line, because both are witnesses.

Is it even a function?

Before either property, the candidate has to be a function. These are examples of how that fails (functions-on-general-sets[290]):

- $f : \mathbb{Z}^+ \to \mathbb{Z}^+$, $f(n) = \frac{(n+1)(n+3)}{3}$ — lands **outside the co-domain** ($n = 1$ gives $\frac{8}{3}$).
- $f : \mathbb{Q} \to \mathbb{Z}$, $f(\frac{m}{n}) = m$ — **one input, two values**: $f\left(\frac{1}{2}\right) = 1$ but $f\left(\frac{2}{4}\right) = 2$, and $\frac{1}{2} = \frac{2}{4}$. A rule that depends on how the input is *written* is not well defined.
- $\{(x, y) : y^2 = x\}$ and $\{(x, y) : x = |y|\}$ — **one input, two values** again: $(4, 2)$ and $(4, -2)$; $(1, 1)$ and $(1, -1)$.

A constant function ($f(x) = 1$) and $f(n) = n!$ on $\mathbb{Z}^+$ are functions; the constant one is neither one-to-one nor onto $\mathbb{R}$, which makes it the fourth panel of Figure 42.

[290] courses/math1061/functions-on-general-sets.pdf

See also

- inverse-functions[291] — what a bijection buys you
- composition-of-functions[292] — how the two properties behave under $g \circ f$
- functions-on-general-sets[293] — the definition, co-domain versus range
- counting-selections[294] — a one-to-one function from an r-element set to an n-element set picks r different images in order, so there are $\frac{n!}{(n-r)!}$ of them
- pigeonhole-principle[295] — no function from a finite set to a smaller one is one-to-one, the pigeonhole principle
- quantified-statements[296] · proof-techniques[297] — why the templates have the shape they have
- 2026-09-07-functions-one-to-one-onto-inverse[298] — Lecture 19
- practice-problems[299] — §25

Partial Order Relations

A partial order is a relation that ranks the elements of a set: it is reflexive, antisymmetric and transitive. If in addition every two elements can be compared, it is a total order. The property that is new here is in antisymmetric-relations[300], and the picture of a partial order is its Hasse diagram[301]. First met in 2026-09-22-partial-order-relations[302].

The definitions

A relation R on a set S is a **partial order relation** if and only if R is

1. Reflexive;
2. Antisymmetric; and
3. Transitive.

If R is a relation on a set S, then two elements $a, b \in S$ are **comparable** if and only if $a \; R \; b$ or $b \; R \; a$.

[291] courses/math1061/inverse-functions.pdf
[292] courses/math1061/composition-of-functions.pdf
[293] courses/math1061/functions-on-general-sets.pdf
[294] courses/math1061/counting-selections.pdf
[295] courses/math1061/pigeonhole-principle.pdf
[296] courses/math1061/quantified-statements.pdf
[297] courses/math1061/proof-techniques.pdf
[298] courses/math1061/2026-09-07-functions-one-to-one-onto-inverse.pdf
[299] courses/math1061/practice-problems.pdf
[300] courses/math1061/antisymmetric-relations.pdf
[301] courses/math1061/hasse-diagrams.pdf
[302] courses/math1061/2026-09-22-partial-order-relations.pdf

A relation R on a set S is a **total order relation** if and only if R is

1. Reflexive;
2. Antisymmetric;
3. Transitive; and
4. Any two elements of S are comparable.

Any total order relation is a partial order relation.
A partial order relation is a total order relation if and only if every two elements are comparable.

The model is $\leq$ on numbers, and it helps to read $a\ R\ b$ as "a is below or equal to b". *Partial* refers to condition 4 being absent. In a partial order some pairs may not be ranked against each other at all. *Partial* does not mean "not total": a total order is a partial order that happens to rank every pair.

Comparable elements

Two elements are comparable when they are **related in some direction**. They are non-comparable when **neither** $a\ R\ b$ **nor** $b\ R\ a$ holds.

Relation	Comparable	Non-comparable
$\subseteq$ on $\mathcal{P}(\mathbb{Z})$	$\{7\}$ and $\{7, 9\}$	$\{7\}$ and $\{9\}$; $\{1, 2, 3\}$ and $\{1, 2, 4\}$
divides on $\mathbb{Z}^+$	2 and 6	2 and 3
$\leq$ on $\mathbb{R}$	every pair	none

The first row is worked in 2026-09-22-partial-order-relations[303].

- **Non-comparable is not "different".** $\{7\}$ and $\{7, 9\}$ are different and comparable.
- **Non-comparable is not "disjoint" or "unlike".** $\{1, 2, 3\}$ and $\{1, 2, 4\}$ share two elements and are still non-comparable, because neither contains the other.
- **Both directions have to fail.** $6 \nmid 2$ on its own does not make 2 and 6 non-comparable, because $2 \mid 6$.
- **The elements have to be in the set.** 7 and 9 are not comparable under $\subseteq$ on $\mathcal{P}(\mathbb{Z})$, and not non-comparable either: they are not elements of $\mathcal{P}(\mathbb{Z})$.

In a partial order every element is comparable with itself, because the relation is reflexive. The definition of comparable applies to any relation, and in a relation that is not reflexive an element is comparable with itself only if it has a loop, as in the six-point example of 2026-09-22-partial-order-relations[304].

[303] courses/math1061/2026-09-22-partial-order-relations.pdf
[304] courses/math1061/2026-09-22-partial-order-relations.pdf

Proving a relation is a partial order

Three labelled parts, as for an equivalence relation (equivalence-relations[305]), with the middle one changed:

Part	Start with	Show
reflexive	Let $a \in S$.	$a \mathrel{R} a$
antisymmetric	Let $a, b \in S$ and suppose $a \mathrel{R} b$ and $b \mathrel{R} a$.	$a = b$
transitive	Let $a, b, c \in S$ and suppose $a \mathrel{R} b$ and $b \mathrel{R} c$.	$a \mathrel{R} c$

Worked: divides on $\mathbb{Z}^+$

The proof is written out in full in 2026-09-22-partial-order-relations[306]. Unfold $a \mid b$ as $b = ak$ for some $k \in \mathbb{Z}$ (divisibility-and-factorisation[307]).

- **Reflexive.** $a = a \cdot 1$, so $a \mid a$.
- **Antisymmetric.** If $b = ak$ and $a = b\ell$ then $b = b(\ell k)$, so $\ell k = 1$. Both are positive, so $\ell = k = 1$ and $a = b$.
- **Transitive.** If $b = ak$ and $c = b\ell$ then $c = a(k\ell)$ and $k\ell \in \mathbb{Z}$, so $a \mid c$.

Worked: $\subseteq$ on a set of sets

Let S be any set of sets, for instance a power set.

- **Reflexive.** Every set is a subset of itself: $X \subseteq X$.
- **Antisymmetric.** If $X \subseteq Y$ and $Y \subseteq X$ then $X = Y$ (sets-and-set-notation[308]).
- **Transitive.** If $X \subseteq Y$ and $Y \subseteq Z$, then every element of X is in Y and so in Z: $X \subseteq Z$.

Proper subset, $\subset$, is **not** a partial order under this definition: it is not reflexive (2026-09-17-relations-reflexivity-symmetry-transitivity[309]). The same goes for $<$ on $\mathbb{R}$. Both are antisymmetric and transitive, and neither has a single loop.

[305] courses/math1061/equivalence-relations.pdf
[306] courses/math1061/2026-09-22-partial-order-relations.pdf
[307] courses/math1061/divisibility-and-factorisation.pdf
[308] courses/math1061/sets-and-set-notation.pdf
[309] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf

Total or not

Once a relation is known to be a partial order, totality is one more "for all": *for all* $a, b \in S$, $a \; R \; b$ *or* $b \; R \; a$.

	How
To show it is total	Let $a, b \in S$. Show that $a \; R \; b$ or $b \; R \; a$, usually by splitting into cases.
To show it is not total	Find **one** pair that is not comparable.

Divides on $\mathbb{Z}^+$ is not total: $2 \nmid 3$ and $3 \nmid 2$. One pair that cannot be compared is the whole answer. With τ for "divides" it is written $2 \not\tau 3$ and $3 \not\tau 2$.

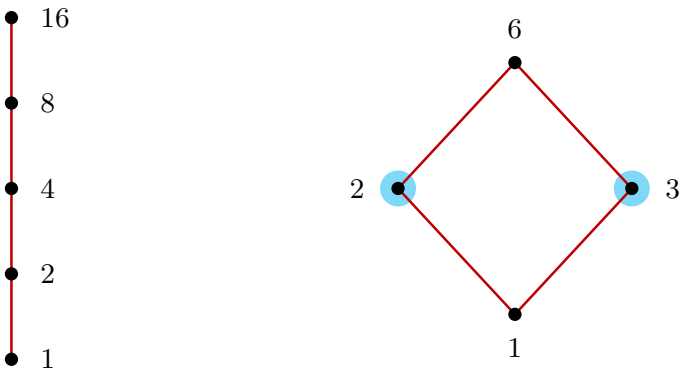
A total order by cases (practice-problems[310], Q1): for $x \; \rho \; y \leftrightarrow x^3 - 1 < y^3$ on $\mathbb{Z}$, take two different integers x, y. Then $x^3 \neq y^3$, so either $x^3 < y^3$, giving $x \; \rho \; y$, or $y^3 < x^3$, giving $y \; \rho \; x$.

Whether an order is total depends on the set. Take "divides" on $\{1, 2, 4, 8, 16\}$. There each number divides all the later ones, every two are comparable, and the order is total. On a set that contains 2 and 3 it is not.

The examples side by side

Relation	on	Partial order?	Total order?
$\leq$	$\mathbb{R}$	**yes**	**yes**
divides	$\mathbb{Z}^+$	**yes**	no: 2 and 3
divides	$\{1, 2, 4, 8, 16\}$	**yes**	**yes**
$\subseteq$	$\mathcal{P}(\{1, 2, 3\})$	**yes**	no: $\{1\}$ and $\{2\}$
$\subseteq$	$\mathcal{P}(\mathbb{Z})$	**yes**	no: $\{7\}$ and $\{9\}$
$x^3 - 1 < y^3$	$\mathbb{Z}$	**yes**	**yes**
five elements in a single column	five elements	**yes**	**yes**
the same with a sixth element at the side	six elements	**yes**	no
weight$(s) \leq$ weight(t)	binary strings of length 6	no: not antisymmetric	—
$<$	$\mathbb{R}$	no: not reflexive	—
divides	$\mathbb{Z}$	no: not antisymmetric	—

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



on $\{1, 2, 4, 8, 16\}$
a total order

on $\{1, 2, 3, 6\}$
partial, not total: $2 \nmid 3$ and $3 \nmid 2$

Figure 43: The relation *divides* on two sets, drawn as Hasse diagrams: a line means the lower number divides the upper one, and so does any path that goes up all the way. Left: on $1, 2, 4, 8, 16$ the diagram is a single column. Any two numbers are joined by an upward path, so every two are comparable and the order is total. Right: on $1, 2, 3, 6$ the diagram branches. 2 and 3, shaded, are not joined by an upward path, since neither divides the other, so the order is partial and not total.

Rows 6 and 9 are Q1 and Q2 of practice-problems[311]. Rows 7 and 8 are the two diagrams of 2026-09-22-partial-order-relations[312].

Equivalence relations and partial orders

The two kinds of relation the course singles out differ in one property.

	Equivalence relation	Partial order
Properties	reflexive, **symmetric**, transitive	reflexive, **antisymmetric**, transitive
Between two different related elements	arrows both ways, always	an arrow one way only, always
What it does to the set	sorts it into classes	ranks it
Its picture	separate clusters, a partition	a Hasse diagram
Standard examples	$=$, congruence mod n, same parity	$\leq$, $\subseteq$, divides on $\mathbb{Z}^+$

[311] courses/math1061/practice-problems.pdf
[312] courses/math1061/2026-09-22-partial-order-relations.pdf

	Equivalence relation	Partial order
Notes	equivalence-relations[313], equivalence-classes-and-partitions[314]	partial-order-relations[315], hasse-diagrams[316]

A relation that is both an equivalence relation and a partial order is symmetric and antisymmetric, so all its arrows are loops (antisymmetric-relations[317]), and reflexive, so it has every loop. It is equality.

Common mistakes

- **Taking "partial order" to mean "not a total order".** Every total order is a partial order.
- **Proving "not symmetric" where "antisymmetric" is wanted.** They are different properties (antisymmetric-relations[318]).
- **Calling $<$ or $\subset$ a partial order.** With this course's definition a partial order is reflexive.
- **Declaring a pair non-comparable after checking one direction.**
- **Showing a relation is total with an example.** "2 and 4 are comparable" proves nothing about every pair. Not total, on the other hand, needs only one pair.
- **Forgetting the set.** Divides is a partial order on $\mathbb{Z}^+$, a total order on $\{1, 2, 4, 8, 16\}$, and not even antisymmetric on $\mathbb{Z}$.

See also

- antisymmetric-relations[319] — the property that separates a partial order from an equivalence relation
- hasse-diagrams[320] — the standard drawing of a partial order
- reflexive-symmetric-and-transitive-relations[321] — reflexive and transitive, with their proof templates
- equivalence-relations[322] — the other important kind of relation

[313] courses/math1061/equivalence-relations.pdf
[314] courses/math1061/equivalence-classes-and-partitions.pdf
[315] courses/math1061/partial-order-relations.pdf
[316] courses/math1061/hasse-diagrams.pdf
[317] courses/math1061/antisymmetric-relations.pdf
[318] courses/math1061/antisymmetric-relations.pdf
[319] courses/math1061/antisymmetric-relations.pdf
[320] courses/math1061/hasse-diagrams.pdf
[321] courses/math1061/reflexive-symmetric-and-transitive-relations.pdf
[322] courses/math1061/equivalence-relations.pdf

- divisibility-and-factorisation[323] · sets-and-set-notation[324] — the two standard partial orders, divides and $\subseteq$
- 2026-09-22-partial-order-relations[325] — Lecture 25
- practice-problems[326] — §32, with full worked solutions

Practice Problems — the Semester-wide Set

This is the course's one problem set for the whole semester — a single document rather than a per-week handout. 46 sections, one per pre-work video, each with the relevant textbook pages, a set of practice problems and full worked solutions. Everything is reproduced here in full, so you never need to open the PDF.

Applied Classes start in **Week 2** and run to Week 13 — twelve of them, matching the "best 8 of 12" Applied Classes component worth 30% (see math1061[327]). Each week's class applies the *previous* week's lecture content, so the material a class covers runs roughly one week behind the lecture column below. Which sections a given Applied Class draws on is not stated in any of the source material.

These problems belong to the roughly three hours of individual study each week, which are for revising the videos, readings and classes **and completing the Practice Problems**. They are the out-of-class half of the course, and they are *not* the same thing as the Assessed Exercises, which are done and submitted inside the class itself. (That class goes by two names, the **Active Class** and the **Applied Class**. They are one session.)

How each section is laid out

1. Relevant textbook pages for Epp 4th edition and 5th (metric) edition
2. **Practice problems**
3. **Solutions** — full worked solutions, not just answers
4. Occasionally a non-assessable **Application** block (see the table below)

Errata

The source document carries an errata page listing corrections made during semester. **Last update: 24 August 2026**, with two entries:

[323] courses/math1061/divisibility-and-factorisation.pdf
[324] courses/math1061/sets-and-set-notation.pdf
[325] courses/math1061/2026-09-22-partial-order-relations.pdf
[326] courses/math1061/practice-problems.pdf
[327] courses/math1061/math1061.pdf

- On page 195, the solution to 1(b) was corrected (the note in brackets had previously copied the note from 1(a)) — already applied in §45 below.
- **Question 2 in section 30 has been updated, and the original version moved to section 32** (because it refers to antisymmetry) — applied in §30 and §32 below.

If something looks wrong, post on the Ed Discussion board.

Section index

Every section is below, with its topic and textbook page ranges. Each section goes with one pre-work video (§1 with *Video 001*, and so on up to *Video 046*), and the Lecture (week) column places it in the schedule of math1061[328] by that video number. The Notes column links to the concept note covering that material where one exists; the rest are still ahead in the semester.

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
1	Logical Form	L2 (wk 1)	023–029	037–043	logical-connectives[329]
2	Logical Equivalence	L2 (wk 1)	030–038	043–053	logical-equivalence-laws[330]
3	Conditional Statements	L3 (wk 1)	039–050	053–066	conditional-statements[331]
4	Valid and Invalid Arguments	L4 (wk 2)	051–063	066–079	valid-argument-forms[332]
5	Methods for Determining Validity	L5 (wk 2)	051–063	066–079	determining-argument-validity[333]
6	Quantified Statements	L5 (wk 2)	096–108	108–121	quantified-statements[334]
7	Negation of Quantified Statements	L6 (wk 2)	108–117	122–131	quantified-statements[335]

[328] courses/math1061/math1061.pdf
[329] courses/math1061/logical-connectives.pdf
[330] courses/math1061/logical-equivalence-laws.pdf
[331] courses/math1061/conditional-statements.pdf
[332] courses/math1061/valid-argument-forms.pdf
[333] courses/math1061/determining-argument-validity.pdf
[334] courses/math1061/quantified-statements.pdf
[335] courses/math1061/quantified-statements.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
8	Statements with Multiple Quantifiers	L6 (wk 2)	117–131	131–146	quantified-statements[336]
9	Direct Proofs and Counterexamples	L7 (wk 3)	145–163	160–182	proof-techniques[337]
10	Proof by Contradiction	L8 (wk 3)	198–207	218–228	proof-techniques[338]
11	Proof by Contraposition	L9 (wk 3)	198–207	218–228	proof-techniques[339]
12	Rational Numbers	L9 (wk 3)	163–170	183–190	rational-and-irrational-numbers[340]
13	Divisibility	L10 (wk 4)	170–179	190–199	divisibility-and-factorisation[341]
14	Modular Arithmetic	L11 (wk 4)	482–485	528–531	modular-arithmetic[342]
15	The Euclidean Algorithm	L12 (wk 4)	220–224	250–254	gcd-lcm-and-euclidean-algorithm[343]
16	Sequences	L13 (wk 5)	227–244	258–275	sequences-and-summations[344]
17	Mathematical Induction	L13 (wk 5)	244–268	275–301	mathematical-induction[345]
18	Strong Induction and the Well Ordering Principle	L14 (wk 5)	268–279	301–314	strong-induction-and-the-well-ordering-principle[346]

[336] courses/math1061/quantified-statements.pdf
[337] courses/math1061/proof-techniques.pdf
[338] courses/math1061/proof-techniques.pdf
[339] courses/math1061/proof-techniques.pdf
[340] courses/math1061/rational-and-irrational-numbers.pdf
[341] courses/math1061/divisibility-and-factorisation.pdf
[342] courses/math1061/modular-arithmetic.pdf
[343] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[344] courses/math1061/sequences-and-summations.pdf
[345] courses/math1061/mathematical-induction.pdf
[346] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
19	Recursive Definitions	L15 (wk 6)	290–304	325–340	recursive-definitions[347]
20	Solving Recurrence Relations	L16 (wk 6)	304–328	340–364	solving-recurrence-relations[348]
21	Set Theory Definitions	L17 (wk 6)	336–351	377–391	sets-and-set-notation[349]
22	More Definitions and Examples of Sets	L17 (wk 6)	336–351	377–391	sets-and-set-notation[350]
23	Properties of Sets	L18 (wk 7)	352–366	391–407	proving-set-properties[351]
24	Functions Defined on General Sets	L18 (wk 7)	383–396	425–439	functions-on-general-sets[352]
25	one-to-one, Onto, and Inverse Functions	L19 (wk 7)	397–416	439–461	
26	Composition of Functions	L20 (wk 7)	416–427	461–472	
27	Cardinalities	L21 (wk 8)	428–441	473–486	
28	Countable and Uncountable Sets	L22 (wk 8)	428–441	473–486	
29	Relations on Sets	L23 (wk 8)	442–449	487–494	
30	Reflexivity, Symmetry, Transitivity	L23 (wk 8)	449–459	495–505	
31	Equivalence Relations	L24 (wk 9)	459–478	505–523	

[347] courses/math1061/recursive-definitions.pdf
[348] courses/math1061/solving-recurrence-relations.pdf
[349] courses/math1061/sets-and-set-notation.pdf
[350] courses/math1061/sets-and-set-notation.pdf
[351] courses/math1061/proving-set-properties.pdf
[352] courses/math1061/functions-on-general-sets.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
32	Partial Order Relations	L25 (wk 9)	498–515	546–563	
33	Definitions and Examples of Groups	L26 (wk 9)	—	—	
34	Elementary Properties of Groups	L27 (wk 10)	—	—	
35	Group Isomorphisms	*not scheduled*	—	—	
36	Definitions and Examples of Fields	L28 (wk 10)	—	—	
37	Introduction to Counting	L29 (wk 11)	516–553	564–604	
38	Counting Selections	L30 (wk 11)	516–553	564–604	
39	Introduction to Probability	L31 (wk 12)	516–553	564–604	
40	Binomial Coefficients	L31 (wk 12)	565–591	617–641	
41	Inclusion Exclusion	L32 (wk 12)	545–549	595–599	
42	The Pigeonhole Principle	L33 (wk 12)	554–565	604–616	
43	Introduction to Graph Theory	L33 (wk 12)	625–660	677–697	
44	Walks, Trails and Circuits	L34 (wk 12)	625–660	677–697	
45	Matrix Representations of Graphs	L35 (wk 13)	661–675	698–712	
46	Trees	L36 (wk 13)	683–701	720–742	

§35 Group Isomorphisms has no lecture in the published schedule — the Week 10 row jumps from L27 (V34) to L28 (V36). The section itself carries no practice problems and is marked *optional and will not be assessed*, so the gap is deliberate.

§28 Countable and Uncountable Sets carries its own note in the source: *this content will not be assessed in MATH1061.* It still has a full set of problems and solutions.

Sections 33–36 (groups and fields) list no textbook page ranges.

Non-assessable application blocks

Eight sections carry an extra block of problems, **not assessable for MATH1061**, mostly drawn from K. Rosen, *Discrete Mathematics and its Applications*, 7th ed. (1991), with two from Epp. They connect the pure material to computer science, and are reproduced in full alongside their sections.

After §	Block	Source
2	Applications to Computer Science — bit strings and logic circuits	Rosen pp. 20–24
5	Applications of Valid and Invalid Arguments	Rosen pp. 48–68
9	Applications of Proofs to Computer Science — resolution and automated theorem proving	Rosen pp. 74–80
15	Trace Tables for Algorithms — the Division and Euclidean algorithms	Epp §4.8 (4th ed.) / §4.10 (5th ed.)
21	Computer Representations of Sets	Rosen pp. 134–138
28	Computability of Functions	Rosen pp. 170–177
31	Identifiers — C identifiers as an equivalence-relation example	Rosen pp. 608–618
37	Runtime — counting basic instructions	Epp 5th ed. pp. 787–799

A note on the diagrams: the source PDF draws logic circuits, graphs and Hasse diagrams as figures. Those are reproduced here as explicit gate netlists and edge lists, which carry the same information in a form that renders everywhere.

§1 — Logical Form

Epp 4th ed. pp. 023–029 · 5th ed. (metric) pp. 037–043. Lecture 2 (week 1). Notes: logical-connectives[353].

Problems

1. Write a truth table for the statement form $p \wedge (\sim q \vee r)$.
2. Suppose you know that $(\sim p \wedge q) \vee p$ is false. What can you conclude about the truth values of each of the two variables?
3. Let p be the statement "DATAENDFLAG is off," q the statement "ERROR equals 0," and r the statement "SUM is less than 1,000." Express the following sentences in symbolic notation.
   (a) DATAENDFLAG is off, ERROR equals 0, and SUM is less than 1,000.
   (b) DATAENDFLAG is off but ERROR is not equal to 0.
   (c) DATAENDFLAG is off; however, ERROR is not 0 or SUM is greater than or equal to 1,000.
   (d) DATAENDFLAG is on and ERROR equals 0 but SUM is greater than or equal to 1,000.
   (e) Either DATAENDFLAG is on or it is the case that both ERROR equals 0 and SUM is less than 1,000.

Solutions

1. The truth table is

p	q	r	$\sim q$	$\sim q \vee r$	$p \wedge (\sim q \vee r)$
T	T	T	F	T	T
T	T	F	F	F	F
T	F	T	T	T	T
T	F	F	T	T	T
F	T	T	F	T	F
F	T	F	F	F	F
F	F	T	T	T	F
F	F	F	T	T	F

[353] courses/math1061/logical-connectives.pdf

2. We know $(\sim p \wedge q) \vee p$ is false. A disjunction is false only when both parts are false, so we must have

$$p \text{ is false} \quad \text{and} \quad (\sim p \wedge q) \text{ is false.}$$

From p being false, it follows that $\sim p$ is true. Now $(\sim p \wedge q)$ can be false only if q is false (since $\sim p$ is already true). Hence q is false.

Therefore p **is false and** q **is false**.

3. (a) $p \wedge q \wedge r$.

(b) $p \wedge \sim q$.

(c) $p \wedge (\sim q \vee \sim r)$.

(d) $\sim p \wedge q \wedge \sim r$.

(e) $\sim p \vee (q \wedge r)$.

§2 — Logical Equivalence

Epp 4th ed. pp. 030–038 · 5th ed. (metric) pp. 043–053. Lecture 2 (week 1). Notes: logical-equivalence-laws[354].

Problems

1. (a) Use the laws of logical equivalence to show that $p \wedge q \equiv \sim (\sim p \vee \sim q)$.

(b) Use the laws of logical equivalence to show that $\sim (p \vee \sim q) \vee (\sim p \wedge \sim q) \equiv \sim p$.

2. For each of the following, write down a truth table for the statement, and determine whether the statement is a tautology, a contradiction, or neither.

(a) $((p \wedge q) \vee (q \wedge r)) \vee \sim q$

(b) $(\sim p \vee q) \vee (p \wedge \sim q)$

3. Use De Morgan's laws to write sentences equivalent to the following:

(a) It is not true that I am studying Computer Science and I am studying Engineering.

(b) I am not going to the movies this weekend or I am not going swimming this weekend.

[354] courses/math1061/logical-equivalence-laws.pdf

4. Let $\oplus$ denote **exclusive or**, which means '… or … but not both'. The truth table for $p \oplus q$ is as follows:

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

   (a) Use a truth table to show that $(p \vee q) \wedge \sim p \equiv q \wedge \sim p$.

   (b) Use a truth table to show that $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$.

   (c) Use the laws of logical equivalence and the equivalence $p \oplus q \equiv (p \vee q) \wedge \sim (p \wedge q)$ (which is the definition of $\oplus$) to show that

$$(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r).$$

Solutions

1. (a) We have

$$\begin{aligned} \sim (\sim p \vee \sim q) &\equiv \sim (\sim p) \wedge \sim (\sim q) && \text{by De Morgan's law} \\ &\equiv p \wedge q && \text{by the double negative law (used twice).} \end{aligned}$$

   (b) We have

$$\begin{aligned} \sim (p \vee \sim q) \vee (\sim p \wedge \sim q) &\equiv (\sim p \wedge \sim\sim q) \vee (\sim p \wedge \sim q) && \text{by De Morgan's law} \\ &\equiv (\sim p \wedge q) \vee (\sim p \wedge \sim q) && \text{by the double negative law} \\ &\equiv \sim p \wedge (q \vee \sim q) && \text{by the distributive law} \\ &\equiv \sim p \wedge \mathbf{t} && \text{by the negation law} \\ &\equiv \sim p && \text{by the identity law.} \end{aligned}$$

2. (a) We have

p	q	r	$p \wedge q$	$q \wedge r$	$(p \wedge q) \vee (q \wedge r)$	$\sim q$	$((p \wedge q) \vee (q \wedge r)) \vee \sim q$
T	T	T	T	T	T	F	T
T	T	F	T	F	T	F	T
T	F	T	F	F	F	T	T
T	F	F	F	F	F	T	T
F	T	T	F	T	T	F	T
F	T	F	F	F	F	F	F
F	F	T	F	F	F	T	T
F	F	F	F	F	F	T	T

Thus the statement is **neither a tautology nor a contradiction**.

(b) We have

p	q	$\sim p$	$\sim p \vee q$	$\sim q$	$p \wedge \sim q$	$(\sim p \vee q) \vee (p \wedge \sim q)$
T	T	F	T	F	F	T
T	F	F	F	T	T	T
F	T	T	T	F	F	T
F	F	T	T	T	F	T

Hence the statement is a **tautology**.

3. (a) Let C be the statement "I am studying Computer Science" and E be the statement "I am studying Engineering." The given statement is $\sim (C \wedge E)$. By De Morgan's law,

$$\sim (C \wedge E) \equiv (\sim C) \vee (\sim E).$$

So an equivalent statement is: "I am not studying Computer Science or I am not studying Engineering."

(b) Let M be the statement "I am going to the movies this weekend" and S be the statement "I am going swimming this weekend." The given sentence is $(\sim M) \vee (\sim S)$. By De Morgan's law (in reverse),

$$(\sim M) \vee (\sim S) \equiv \sim (M \wedge S).$$

So an equivalent statement is: "It is not the case that I am both going to the movies this weekend and going swimming this weekend."

4. (a) We have

p	q	$p \vee q$	$\sim p$	$(p \vee q) \wedge \sim p$	$q \wedge \sim p$
T	T	T	F	F	F
T	F	T	F	F	F
F	T	T	T	T	T
F	F	F	T	F	F

Since the last two columns agree on every row, we have $(p \vee q) \wedge \sim p \equiv q \wedge \sim p$.

(b) We have

p	q	r	$p \oplus q$	$(p \oplus q) \wedge r$	$p \wedge r$	$q \wedge r$	$(p \wedge r) \oplus (q \wedge r)$
T	T	T	F	F	T	T	F
T	T	F	F	F	F	F	F
T	F	T	T	T	T	F	T
T	F	F	T	F	F	F	F
F	T	T	T	T	F	T	T
F	T	F	T	F	F	F	F
F	F	T	F	F	F	F	F
F	F	F	F	F	F	F	F

The columns for $(p \oplus q) \wedge r$ and $(p \wedge r) \oplus (q \wedge r)$ match on all rows, hence $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$.

(c) To save space, multiple laws have been applied in some steps. There are many different ways to apply the laws to prove this, so your proof may look different to this one. We have

$(p \wedge r) \oplus (q \wedge r)$

$\equiv ((p \wedge r) \vee (q \wedge r)) \wedge \sim ((p \wedge r) \wedge (q \wedge r))$	by the given equivalence (def of $\oplus$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge r) \wedge (q \wedge r))$	by distributive and commutative laws (for $\wedge r$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge q) \wedge (r \wedge r))$	by associative and commutative laws (for $\wedge$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge q) \wedge r)$	by idempotent law
$\equiv (p \vee q) \wedge r \wedge (\sim (p \wedge q) \vee \sim r)$	by De Morgan's law
$\equiv (p \vee q) \wedge \Big((r \wedge \sim (p \wedge q)) \vee (r \wedge \sim r) \Big)$	by distributive law (for $r \wedge$)
$\equiv (p \vee q) \wedge \Big((r \wedge \sim (p \wedge q)) \vee \mathbf{c} \Big)$	by negation law
$\equiv (p \vee q) \wedge r \wedge \sim (p \wedge q)$	by identity law
$\equiv (p \vee q) \wedge \sim (p \wedge q) \wedge r$	by associative and commutative laws (for $\wedge$)
$\equiv (p \oplus q) \wedge r$	by the given equivalence (def of $\oplus$)

Application — Applications to Computer Science

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 20–24.*

Information is often represented using binary or **bit strings**, which are sequences consisting of zeros and ones. The **length** of a string is the total number of bits in it — for example 0110110 is a string of length 7. The logical operators $\wedge$, $\vee$ and $\oplus$ extend to binary strings. The operators AND, OR and XOR are:

p	q	$p \vee q$	$p \wedge q$	$p \oplus q$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Propositional logic also applies to the design of computer hardware. A **digital logic circuit** receives input signals (either 0, the wire being off, or 1, on) and produces output signals which are also bits. Complicated digital logic circuits can be constructed from three basic gates: the **OR gate**, the **NOT gate** and the **AND gate**.

A **combinational circuit** uses these gates and obeys the following rules.

1. Two input wires cannot be combined without a gate.
2. A single input wire can be split partway and directed into two separate gates.
3. An output wire from a gate can be used as input for another gate.

4. No output wire from a gate can eventually feed back into that gate.

For example, the logical expression $(p \wedge \sim q) \vee \sim r$ has the combinational circuit

- NOT$(q) \to n_1$
- AND$(p, n_1) \to a_1$
- NOT$(r) \to n_2$
- OR$(a_1, n_2) \to$ output $(p \wedge \sim q) \vee \sim r$

Application problems

1. Find the bitwise OR, bitwise AND and bitwise XOR of each of these pairs of binary strings.

   (a) 1011110, 0100001

   (b) 11110000, 10101010

2. Construct a combinational circuit using the NOT, OR and AND gates that produces the outputs:

   (a) $(\sim p \vee \sim r) \wedge q$

   (b) $(p \wedge \sim r) \vee (\sim q \wedge r)$

3. Find the output of the following combinational circuit, simplify the expression using logical laws and construct a new circuit for the simplified expression. The circuit is

   - NOT$(p) \to n_1$
   - NOT$(q) \to n_2$
   - OR$(p, n_2) \to o_1$
   - OR$(n_1, n_2) \to o_2$
   - AND$(o_1, o_2) \to a_1$
   - OR$(a_1, r) \to$ output

   (both p and q have their wires split, feeding two gates each).

4. The logical binary operation NAND, denoted $|$, is defined by

$$p \mid q \equiv \sim (p \wedge q).$$

   (a) Write down the truth table for $\sim (p \mid q)$. Show all working.

   (b) Prove, using truth tables or otherwise, that $(p \mid p) \equiv (\sim p)$. Show all working.

   (c) Prove, using truth tables or otherwise, that $((p \mid p) \mid (q \mid q)) \equiv p \vee q$. Show all working.

Application solutions

1. (a)
$$1011110 \text{ OR } 0100001 = 1111111,$$
$$1011110 \text{ AND } 0100001 = 0000000,$$
$$1011110 \text{ XOR } 0100001 = 1111111.$$

   (b)
$$11110000 \text{ OR } 10101010 = 11111010,$$
$$11110000 \text{ AND } 10101010 = 10100000,$$
$$11110000 \text{ XOR } 10101010 = 01011010.$$

2. (a) The circuit is
   - NOT$(p) \to n_1$
   - NOT$(r) \to n_2$
   - OR$(n_1, n_2) \to o_1$
   - AND$(o_1, q) \to$ output $(\sim p \vee \sim r) \wedge q$

   (b) The circuit is
   - NOT$(r) \to n_1$
   - AND$(p, n_1) \to a_1$
   - NOT$(q) \to n_2$
   - AND$(n_2, r) \to a_2$
   - OR$(a_1, a_2) \to$ output $(p \wedge \sim r) \vee (\sim q \wedge r)$

3. The given digital logic circuit has output $((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee r$. Using laws of logical equivalence we have

$$\begin{aligned} ((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee r &\equiv (\sim q \vee (p \wedge \sim p)) \vee r && \text{by distributive and commutative laws} \\ &\equiv (\sim q \vee \mathbf{c}) \vee r && \text{by negation law} \\ &\equiv \sim q \vee r && \text{by identity law} \end{aligned}$$

   The simplification is $\sim q \vee r$. The simplified logic circuit is
   - NOT$(q) \to n_1$
   - OR$(r, n_1) \to$ output $\sim q \vee r$

4. (a) We have

p	q	$p \wedge q$	$p \mid q$	$\sim (p \mid q)$
T	T	T	F	T
T	F	F	T	F
F	T	F	T	F
F	F	F	T	F

Hence $\sim (p \mid q)$ has the same truth values as $p \wedge q$ (it is true exactly when both p and q are true).

(b) Since $p \mid p \equiv \sim (p \wedge p)$, we have

$$p \mid p \equiv \sim (p \wedge p) \equiv \sim p$$

because $p \wedge p \equiv p$ (idempotent law). Alternatively, by truth table:

p	$p \wedge p$	$p \mid p$	$\sim p$
T	T	F	F
F	F	T	T

The last two columns agree, so $p \mid p \equiv \sim p$.

(c) First note from part (b) that $p \mid p \equiv \sim p$ and $q \mid q \equiv \sim q$. Therefore

$$\begin{aligned} (p \mid p) \mid (q \mid q) &\equiv (\sim p) \mid (\sim q) && \text{by part (b)} \\ &\equiv \sim ((\sim p) \wedge (\sim q)) && \text{by def of NAND} \\ &\equiv p \vee q && \text{by De Morgan's law.} \end{aligned}$$

Alternatively, by truth table:

p	q	$p \mid p$	$q \mid q$	$(p \mid p) \mid (q \mid q)$	$p \vee q$
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	F	F

The last two columns match, hence $(p \mid p) \mid (q \mid q) \equiv p \vee q$.

§3 — Conditional Statements

Epp 4th ed. pp. 039–050 · 5th ed. (metric) pp. 053–066. Lecture 3 (week 1). Notes: conditional-statements[355].

Problems

1. Let p, q and r be statements. Use the laws of logical equivalence to show that

$$p \to (q \vee r) \equiv (p \wedge \sim q) \to r.$$

2. Let p and q be statement variables. Are the following statements logically equivalent? Justify your answer.

   - **Statement A:** $(p \to q) \wedge \sim q$
   - **Statement B:** $\sim (p \wedge q)$

3. Write each of the following statements in the form 'if … then …'.

   (a) A sufficient condition for the warranty to be good is that you bought the computer less than a year ago.

   (b) Jane gets seasick whenever she is on a boat.

4. For each of the following, write down a truth table for the statement, and determine whether the statement is a tautology, a contradiction, or neither.

   (a) $(\sim p \wedge (p \to q)) \to \sim q$

   (b) $(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$

5. Negate the following two statements.

   (a) If it rains, then Sue takes her umbrella.

   (b) The cakes burn if the oven temperature is too high.

6. Recall "a sufficient condition for s is r" means r is a sufficient condition for s, and that "a necessary condition for s is r" means r is a necessary condition for s. Rewrite the following statements in 'if … then …' form:

   (a) A sufficient condition for John's team to win the championship is that it wins the rest of its games.

   (b) A necessary condition for this computer program to be correct is that it not produce error messages during translation.

[355] courses/math1061/conditional-statements.pdf

Solutions

1. We have

$$\begin{aligned} p \to (q \vee r) &\equiv \sim p \vee (q \vee r) && \text{by definition of implication} \\ &\equiv (\sim p \vee q) \vee r && \text{by the associative law} \\ &\equiv \sim (p \wedge \sim q) \vee r && \text{by De Morgan's law and double negative law} \\ &\equiv (p \wedge \sim q) \to r && \text{by definition of implication.} \end{aligned}$$

2. Let A be the statement $(p \to q) \wedge \sim q$ and let B be the statement $\sim (p \wedge q)$. Then

$$\begin{aligned} A &\equiv (\sim p \vee q) \wedge \sim q && \text{by definition of implication} \\ &\equiv (\sim p \wedge \sim q) \vee (q \wedge \sim q) && \text{by distributive and commutative laws} \\ &\equiv (\sim p \wedge \sim q) \vee \mathbf{c} && \text{by negation law} \\ &\equiv \sim p \wedge \sim q && \text{by identity law,} \end{aligned}$$

   while

$$B \equiv \sim (p \wedge q) \equiv \sim p \vee \sim q \qquad \text{by De Morgan's law.}$$

   Thus Statement A and Statement B are **not** logically equivalent because, for example, if p is false and q is true, then A is false and B is true. Hence $A \not\equiv B$.

3. (a) If you bought the computer less than a year ago, then the warranty is good.

   (b) If Jane is on a boat, then Jane gets seasick.

4. (a) **Solution Option 1.** The truth table for the statement is

p	q	$\sim p$	$p \to q$	$\sim p \wedge (p \to q)$	$\sim q$	$(\sim p \wedge (p \to q)) \to \sim q$
T	T	F	T	F	F	T
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T

   The statement is **neither a tautology nor a contradiction**.

   Solution Option 2. The same truth table, written under the parts of the statement:

p	q	$\sim p$	$\wedge$	$(p \to q)$	$\to$	$\sim q$
T	T	F	F	T	T	F
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T
order						

The small numbers show the order in which the columns were completed. Column comes from comparing columns and . Column comes from comparing columns and , and shows the truth values for the entire statement. This shows that this statement is neither a tautology nor a contradiction. (You don't have to number the columns — this is just to help your understanding!)

(b) **Solution Option 1.** The truth tables for the LHS and RHS are:

p	q	r	$q \vee r$	$p \to (q \vee r)$	$\sim q$	$p \wedge \sim q$	$(p \wedge \sim q) \to r$
T	T	T	T	T	F	F	T
T	T	F	T	T	F	F	T
T	F	T	T	T	T	T	T
T	F	F	F	F	T	T	F
F	T	T	T	T	F	F	T
F	T	F	T	T	F	F	T
F	F	T	T	T	T	F	T
F	F	F	F	T	T	F	T

Therefore the truth table for the statement is:

p	q	r	$(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T

The statement is a **tautology**.

Solution Option 2. Another way to represent the truth table for $(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$:

p	q	r	$p \to$	$(q \vee r)$	$\leftrightarrow$	$(p \wedge \sim q)$	$\to r$
T	T	T	T	T	T	F	T
T	T	F	T	T	T	F	T
T	F	T	T	T	T	T	T
T	F	F	F	F	T	T	F
F	T	T	T	T	T	F	T
F	T	F	T	T	T	F	T
F	F	T	T	T	T	F	T
F	F	F	T	F	T	F	T
order							

Here column comes from comparing columns and . We see (from column) that this is a tautology.

5. (a) Let R be the statement "it rains" and U be the statement "Sue takes her umbrella." The given statement is $R \to U$. Its negation is

$$R \wedge \sim U,$$

i.e. "It rains and Sue does not take her umbrella."

(b) Let H be the statement "the oven temperature is too high" and B be the statement "the cakes burn." The given statement is $H \to B$. Its negation is

$$H \wedge \sim B,$$

i.e. "The oven temperature is too high and the cakes do not burn."

6. (a) If John's team wins the rest of its games, then John's team will win the championship.

(b) If this computer program is correct, then it does not produce error messages during translation.

§4 — Valid and Invalid Arguments

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 4 (week 2). Notes: valid-argument-forms[356].

[356] courses/math1061/valid-argument-forms.pdf

Problems

1. State truth values for the statement variables p and q that demonstrate that the following argument is invalid, and justify your answer.

   Premise 1: q Premise 2: $p \to q$ Conclusion: p

2. Find values of the statement variables a, b and c that show that the following argument is invalid.

   1. $a \to b$
   2. $\sim a \to c$
   3. $\sim b \to c \therefore b$

3. Use a truth table to show that the following argument forms are valid.

   (a) **Elimination:**

   1. $p \vee q$
   2. $\sim q \therefore p$

   (b) **Generalisation:**

   1. $p \therefore p \vee q$

4. Use a truth table to show that the following argument is invalid.

   1. $(p \wedge q) \to \sim r$
   2. $p \vee \sim q$
   3. $\sim q \to p \therefore \sim r$

Solutions

1. To show the argument is invalid, we must find truth values for p and q such that the premises are true and the conclusion is false.

   Suppose p is false and q is true. Then Premise 1 (q) is true and Premise 2 ($p \to q$) is true (by definition of implication). However, the conclusion (p) is false. Therefore the argument is invalid.

2. To show the argument is invalid, we must find truth values for a, b and c such that the premises are true and the conclusion is false.

   Let a be false, b be false, and c be true. By definition of implication, all three premises are true, but the conclusion (b) is false, so the argument is invalid.

3. (a)

p	q	premise 1: $p \vee q$	premise 2: $\sim q$	conclusion: p
T	T	T	F	T
T	F	T	T	T
F	T	T	F	F
F	F	F	T	F

There is only one row of the truth table in which all premises are true (the second row), and here the conclusion is true. Thus, whenever all the premises are true, the conclusion is true, so the argument is **valid**.

(b)

p	q	premise 1: p	conclusion: $p \vee q$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	F	F

There are two rows for which all premises (here just the one premise) are true — the first two rows — and for each of these rows the conclusion is true. Thus, whenever all the premises are true, the conclusion is true, so the argument is **valid**.

4. We compute the truth table:

p	q	r	$(p \wedge q) \rightarrow \sim r$	$p \vee \sim q$	$\sim q \rightarrow p$	Prem. 1 $\wedge$ Prem. 2 $\wedge$ Prem. 3	$\sim r$
T	T	T	F	T	T	F	F
T	T	F	T	T	T	T	T
T	F	T	T	T	T	T	F
T	F	F	T	T	T	T	T
F	T	T	T	F	T	F	F
F	T	F	T	F	T	F	T
F	F	T	T	T	F	F	F
F	F	F	T	T	F	F	T

There are three rows for which all the premises are true, however for one of these rows the conclusion is false. In particular, taking p to be true, q to be false, and r to be true makes all the premises true but the conclusion false, so the argument is **invalid**.

§5 — Methods for Determining Validity

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 5 (week 2). Notes: determining-argument-validity[357].

Problems

1. Determine whether the following arguments are valid. If the argument is valid, prove it using rules of inference. If the argument is invalid, demonstrate it with a choice of truth values for the variables.

   (a)

   $p \to q \; q \to p \therefore p \vee q$

   (b)

   $p \; p \to q \sim q \vee r \therefore r$

   (c)

   $p \vee q \; p \to\sim q \; p \to r \therefore r$

2. Write the following argument in symbolic form. Then determine whether the argument is valid or not.

   > An error message is received if the output is flagged. The system is running normally only if the output is not flagged. An error message is received. Therefore, the system is not running normally.

   Please use the following variables:

p	the output is flagged
q	an error message is received
r	the system is running normally

[357] courses/math1061/determining-argument-validity.pdf

3. Give truth values for the variables p, q, r, s and w which demonstrate that the following argument is invalid.

$$\big[(p \vee q) \wedge (q \to r) \wedge ((p \wedge s) \to w) \wedge (\sim r) \wedge (q \to s)\big] \to w$$

Solutions

1. (a) The argument is **invalid**. When p and q are both false, all the premises are true, but the conclusion is false. One could arrive at this example by computing the following truth table:

p	q	$p \to q$	$q \to p$	$p \vee q$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	F

(In the last row, the premises are true, but the conclusion is false.)

(b) The argument is **valid**, and we prove this with rules of inference:

1.	p	Premise
2.	$p \to q$	Premise
3.	$\sim q \vee r$	Premise
4.	q	from 1 and 2 by Modus Ponens
5.	r	from 3 and 4 by elimination (and the double negative law)

Therefore the argument is valid.

(c) Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have r **is false**. Since r is false but the third premise $(p \to r)$ is true, we must have p **is false**. Since p is false, this means the second premise $(p \to \sim q)$ is also true. Now since p is false but the first premise $(p \vee q)$ is true, we must have q **is true**.

Thus, with these truth values for the three variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

2. The argument has the symbolic form:

1.	$p \to q$	(An error message is received if the output is flagged.)
2.	$r \to \sim p$	(The system is running normally only if the output is not flagged.)
3.	q	(An error message is received.)
$\therefore$	$\sim r$	(The system is not running normally.)

Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have r **is true**. Since r is true, and premise 2 is true, we must have $\sim p$ true, that is p **is false**. Since premise 3 is true, we have q **is true**.

Thus, with these truth values for the three variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

3. The argument being valid is the same as this overall implication statement being a tautology.

$$\big[(p \vee q) \wedge (q \to r) \wedge ((p \wedge s) \to w) \wedge (\sim r) \wedge (q \to s)\big] \to w$$

We can write the argument as follows:

1. $p \vee q$
2. $q \to r$
3. $(p \wedge s) \to w$
4. $\sim r$
5. $q \to s \therefore w$

Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have w **is false**. Since premise 4 is true we have r **is false**. Since premise 2 is true and r is false, we must have q **is false**. Since premise 1 is true and q is false we have p **is true**. Since premise 3 is true and w is false, we must have $(p \wedge s)$ false, and since p is true, this means s **is false**. These truth values also mean premise 5 is true.

Thus with these truth values for the variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

Application — Applications of Valid and Invalid Arguments

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 48–68.*

Application problems

1. Translating English sentences into logical expressions is an essential part of specifying both hardware and software systems. Software engineers must take requirements in English and produce precise, unambiguous specifications that can be used as the basis for system development.

   Consider the following predicates and domains:

   Predicates:

$F(x, y)$	disk x has more than y kilobytes of free space.
$S(m)$	mail message m can be saved.
$A(x)$	alert x is active.
$Q(m)$	message m is queued.
$T(m)$	message m is transmitted.
$D(s)$	the diagnostic monitor tracks the status of system s.

   Domains:

M	the nonempty set of all messages.
X	the set of all disks.
Y	the set of all alerts.
S	the set of all systems.

   Express the system specifications below using quantifiers and logical connectives:

   (a) At least one mail message, among the nonempty set of messages, can be saved if there is a disk with more than 10 kilobytes of free space.

   (b) Whenever there is an active alert, all queued messages are transmitted.

   (c) The diagnostic monitor tracks the status of all systems except the main console.

2. System specifications should be **consistent**; that is, they should not contain conflicting requirements that could be used to derive a contradiction. When specifications are not consistent, there would be no way to develop a system that satisfies all specifications. Logically, a system is consistent if it is possible for all the premises to be simultaneously true.

Use logical expressions and methods of logical deduction to determine whether the following specifications are consistent.

(a) The system is in multiuser state if and only if it is operating normally. If the system is operating normally, the kernel is functioning. The kernel is not functioning or the system is in interrupt mode. If the system is not in multiuser state, then it is in interrupt mode. The system is not in interrupt mode.

(b) The router can send packets to the edge system only if it supports the new address space. For the router to support the new address space it is necessary that the latest software release be installed. The router can send packets to the edge system if the latest software release is installed. The router does not support the new address space.

Application solutions

1. (a) $(\exists x \in X \text{ s.t. } F(x, 10)) \rightarrow (\exists m \in M \text{ s.t. } S(m))$.

   (b) $(\exists y \in Y \text{ s.t. } A(y)) \rightarrow (\forall m \in M,\ (Q(m) \rightarrow T(m)))$.

   (c) Let $c \in S$ denote the main console. $\forall s \in S,\ (s \neq c \rightarrow D(s))$.

2. (a) Define the following variables:

m	the system is in multiuser state
n	the system is operating normally
k	the kernel is functioning
i	the system is in interrupt mode

Now we can express the specifications as follows:

1. $m \leftrightarrow n$
2. $n \rightarrow k$
3. $\sim k \vee i$
4. $\sim m \rightarrow i$
5. $\sim i$

Solution Option 1. If these specifications are consistent, then we must be able to find truth values for each of the variables that makes all of the specifications true. Assume the specifications are consistent (so we assume each specification is true). For specification 5 to be true we know i **is false**. For specification 4 to be true, with i false, we know $\sim m$ is false so m **is true**. For premise 1 to be true, with m true, we have n **is true**. For specification 2 to be true, and since n is true, we have k **is true**. However, now $\sim k$ is

false and i is false, which means specification 3 is false. This contradicts our assumption that all the specifications are true, and so it is impossible for the system to be consistent. Therefore, the system is **not consistent**.

Solution Option 2. Suppose the specifications are all true. Using laws of inference, we have

1.	$m \leftrightarrow n$	specification
2.	$n \rightarrow k$	specification
3.	$\sim k \vee i$	specification
4.	$\sim m \rightarrow i$	specification
5.	$\sim i$	specification
6.	$\sim k$	from 3 and 5 by elimination (and double negative law)
7.	$\sim n$	from 2 and 6 by Modus Tollens
8.	$(m \rightarrow n) \wedge (n \rightarrow m)$	from 1 by definition of $\leftrightarrow$
9.	$m \rightarrow n$	from 8 by specialisation
10.	$\sim m$	from 9 and 7 by Modus Tollens
11.	i	from 4 and 10 by Modus Ponens

But now we have both i and $\sim i$ being true, which is a contradiction. This contradicts our assumption that all the specifications are true, and so it is impossible for the system to be consistent. Therefore, the system is **not consistent**.

(b) Define the following variables:

r	the router can send packets to the edge system
a	the router supports the new address space
s	the latest software release is installed

Now we can express the specifications as follows:

1. $r \rightarrow a$
2. $a \rightarrow s$
3. $s \rightarrow r$
4. $\sim a$

Assume the specifications are consistent, so each specification is true. For specification 4 to be true, $\sim a$ is true, so a **is false**. For specification 1 to be true with a false we must

have r **is false**. Now, since r is false and specification 3 is true, we have s **is false**. We double-check that specification 2 is true, which it is because a is false. Thus, we have found truth values of the statement variables that make all of the specifications true, so the system **is consistent**.

§6 — Quantified Statements

Epp 4th ed. pp. 096–108 · 5th ed. (metric) pp. 108–121. Lecture 5 (week 2). Notes: quantified-statements[358].

Problems

1. Rewrite each of the following in the form "∀__, __." Here, let D be the set of all dinosaurs, and let L be the set of all logicians.
   (a) All dinosaurs are extinct.
   (b) Every real number is positive, negative, or zero.
   (c) No irrational numbers are integers.
   (d) No logicians are lazy.
   (e) The number 2,147,581,953 is not equal to the square of any integer.
   (f) The number -1 is not equal to the square of any real number.
2. Rewrite each of the following in the form "∃__ such that __." Here, let X be the set of all exercises.
   (a) Some exercises have answers.
   (b) Some real numbers are rational.
3. Determine whether the following statements are true or false. Justify your reasoning.
   (a) $\forall x \in \mathbb{R},\ x \geq \frac{1}{x}$.
   (b) $\forall a \in \mathbb{Z},\ \frac{a-1}{a} \notin \mathbb{Z}$.
   (c) $\forall m, n \in \mathbb{Z}^+,\ mn \geq m + n$.

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

Solutions

1. (a) $\forall x \in D,\ x$ is extinct.

   (b) $\forall x \in \mathbb{R},\ (x > 0 \vee x < 0 \vee x = 0)$.

   (c) $\forall x \in \mathbb{R},\ (x \text{ is irrational} \to x \notin \mathbb{Z})$.

   (d) $\forall x \in L,\ x$ is not lazy.

   (e) $\forall x \in \mathbb{Z},\ x^2 \neq 2147581953$.

   (f) $\forall x \in \mathbb{R},\ -1 \neq x^2$.

2. (a) $\exists x \in X$ such that x has an answer.

   (b) $\exists x \in \mathbb{R}$ such that $x \in \mathbb{Q}$.

3. (a) **False.** Counterexample: take $x = \frac{1}{2}$. Then $x = \frac{1}{2}$ but $\frac{1}{x} = 2$, so $x \geq \frac{1}{x}$ is false.

   (b) **False.** Counterexample: take $a = 1$. Then $\frac{a-1}{a} = \frac{0}{1} = 0 \in \mathbb{Z}$.

   (c) **False.** Counterexample: take $n = m = 1$. Then $mn = 1$ but $m + n = 2$.

§7 — Negation of Quantified Statements

Epp 4th ed. pp. 108–117 · 5th ed. (metric) pp. 122–131. Lecture 6 (week 2). Notes: quantified-statements[359]*.*

Problems

1. Write the negation of each of the following statements, and then determine whether the original or the negation is true:

   (a) $\forall x \in \mathbb{R}$, if $x^2 > 9$ then $x \geq 2$.

   (b) $\forall n \in \mathbb{Z}^+$, n is either prime or composite.

   (c) $\exists x, y \in \mathbb{R}$ such that $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ but $xy \in \mathbb{Z}$.

2. Write down the negation of each of the following statements:

   (a) All fire engines are red.

   (b) Some apples are ripe.

   (c) A triangle with equal sides exists.

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

Solutions

1. (a) **Original:** $\forall x \in \mathbb{R}$, if $x^2 > 9$ then $x \geq 2$. **Negation:** $\exists x \in \mathbb{R}$ such that $x^2 > 9$ and $x < 2$.

   The original statement is **false**. For instance, take $x = -4$. Then $x^2 > 9$ but $x \not\geq 2$.

   (b) **Original:** $\forall n \in \mathbb{Z}^+$, n is either prime or composite. **Negation:** $\exists n \in \mathbb{Z}^+$ such that n is neither prime nor composite.

   The original statement is **false**. For instance, consider $n = 1$, which is neither prime nor composite.

   (c) **Original:** $\exists x, y \in \mathbb{R}$ such that $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ but $xy \in \mathbb{Z}$. **Negation:** $\forall x, y \in \mathbb{R}$, if $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ then $xy \notin \mathbb{Z}$.

   The original statement is **true**. For instance, take $x = \sqrt{2}$ and $y = \sqrt{2}$. Then $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$, but $xy = 2 \in \mathbb{Z}$.

2. (a) **Original:** All fire engines are red. **Negation:** There exists a fire engine which is not red.

   (b) **Original:** Some apples are ripe. **Negation:** All apples are not ripe.

   (c) **Original:** A triangle with equal sides exists. **Negation:** There does not exist a triangle with equal sides.

§8 — Statements with Multiple Quantifiers

Epp 4th ed. pp. 117–131 · 5th ed. (metric) pp. 131–146. Lecture 6 (week 2). Notes: quantified-statements[360].

Problems

1. Write down the negation of each of the following statements. Then determine whether the statement is true, or whether its negation is true.

   (a) $\forall x, y \in \mathbb{Z}$, $\exists z \in \mathbb{Z}$ such that $z = x - y$.

   (b) $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $x^2 - xy - 2y^2 = 0$.

   (c) $\exists x \in \mathbb{Z}^+$ such that $\forall y \in \mathbb{Z}^+$, $x \geq y$.

   (d) $\forall r, s \in \mathbb{R}$, if $rs \in \mathbb{Q}$, then $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$.

2. For each of the following English sentences:

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

(a) For any rational number x and any negative integer y there exists a real number that is greater than the product of x and y.

(b) For every real number x, there is a real number y for which $3y = x$.

do the following:

i. Write the statement in symbolic form.

ii. Write the negation of the statement in symbolic form.

iii. Determine which of the statement or its negation is true.

Solutions

1. (a) **Original:** $\forall x, y \in \mathbb{Z}$, $\exists z \in \mathbb{Z}$ such that $z = x - y$. **Negation:** $\exists x \in \mathbb{Z}$ $\exists y \in \mathbb{Z}$ such that $\forall z \in \mathbb{Z}$, $z \neq x - y$.

The original statement is **true** (and the negation is false). For any given $x, y \in \mathbb{Z}$, choose $z = x - y \in \mathbb{Z}$.

(b) **Original:** $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $x^2 - xy - 2y^2 = 0$. **Negation:** $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}$, $x^2 - xy - 2y^2 \neq 0$.

The original statement is **true** (and the negation is false). For any $x \in \mathbb{R}$, taking $y = \frac{x}{2}$ gives

$$x^2 - x\left(\frac{x}{2}\right) - 2\left(\frac{x}{2}\right)^2 = x^2 - \frac{x^2}{2} - 2 \cdot \frac{x^2}{4} = x^2 - \frac{x^2}{2} - \frac{x^2}{2} = 0.$$

(c) **Original:** $\exists x \in \mathbb{Z}^+$ such that $\forall y \in \mathbb{Z}^+$, $x \geq y$. **Negation:** $\forall x \in \mathbb{Z}^+$ $\exists y \in \mathbb{Z}^+$ such that $x < y$.

The **negation** is true (and the original is false). For any $x \in \mathbb{Z}^+$, take $y = x + 1$. Then y is an integer satisfying the inequality $x < y$.

(d) **Original:** $\forall r, s \in \mathbb{R}$, if $rs \in \mathbb{Q}$, then $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$. **Negation:** $\exists r, s \in \mathbb{R}$ such that $rs \in \mathbb{Q}$ and ($r \notin \mathbb{Q}$ or $s \notin \mathbb{Q}$).

The **negation** is true (and the original is false). Take $r = \sqrt{2}$ and $s = \sqrt{2}$. Then $rs = 2 \in \mathbb{Q}$ but $r, s \notin \mathbb{Q}$.

2. (a) i. **Original:** $\forall x \in \mathbb{Q}$, $\forall y \in \mathbb{Z}^{<0}$, $\exists z \in \mathbb{R}$ s.t. $z > xy$.

ii. **Negation:** $\exists x \in \mathbb{Q}$ $\exists y \in \mathbb{Z}^{<0}$ s.t. $\forall z \in \mathbb{R}$, $z \leq xy$.

iii. The **original** statement is true. For any given $x \in \mathbb{Q}$ and $y \in \mathbb{Z}^{<0}$, take $z = xy + 1$. This is a real number satisfying the inequality $z > xy$.

(b) i. **Original:** $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}$ s.t. $3y = x$.

ii. **Negation:** $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R},\ 3y \neq x$.

iii. The **original** statement is true. Given any $x \in \mathbb{R}$, choose $y = \frac{x}{3}$. This is a real number satisfying the equality $3y = x$.

§9 — Direct Proofs and Counterexamples

Epp 4th ed. pp. 145–163 · 5th ed. (metric) pp. 160–182. Lecture 7 (week 3). Notes: proof-techniques[361].

Problems

1. For each of the following statements, either prove the statement or disprove it using a counterexample.

   (a) The sum of any pair of even integers is even.

   (b) There exist positive integers a, b and c such that $a^2 + b^2 = c^2$.

   (c) There is an even integer n such that $5n - 4$ is prime.

   (d) $\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.

   (e) $\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.

2. Find a counterexample that disproves the following statement:

   $$\text{For all } x \in \mathbb{R},\ \lfloor x^2 \rfloor = \lfloor x \rfloor^2.$$

   (Recall that $\lfloor \cdot \rfloor$ denotes the floor function.)

3. Find the errors in the following proofs and rewrite the proof correctly. Here is a list of common errors made when writing proofs:

   - Arguing from examples
   - Using the same variable to mean two different things
   - Jumping to the conclusion
   - Assuming what is to be proved
   - Confusion between what is known and what is to be shown
   - Use of the word *any* instead of *some*
   - Misuse of the word *if*

[361] courses/math1061/proof-techniques.pdf

(a) The difference between any odd integer and any even integer is odd.

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

(b) If a and b are even integers, then $4a + 2b$ is even.

Proof. We have $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Then we want to show that $4a + 2b$ is even, so

$$\begin{aligned} 4a + 2b &= 2\ell \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

therefore the statement is true.

(c) $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $xy = 1$.

Proof. This is true, for example if $x = 10$ then let $y = \frac{1}{10}$ and $xy = 10 \cdot \frac{1}{10} = 1$. Therefore the statement is true.

(d) $\forall n \in \mathbb{Z}$, if $n > 0$ then $n^2 + 2n + 1$ is composite.

Proof. Suppose n is an integer and $n > 0$, then we want to show that $n^2 + 2n + 1$ is composite, so this means

$$n^2 + 2n + 1 = rs$$

where

$$1 < r, s < n^2 + 2n + 1$$

Clearly neither r nor s are equal to 1 so $n^2 + 2n + 1$ is not prime and hence must be composite.

Solutions

1. (a) **The sum of any pair of even integers is even.**

Proof. Let $m, n \in \mathbb{Z}$ be even. Then $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Hence

$$m + n = 2k + 2\ell = 2(k + \ell),$$

which is even. Therefore, the sum of any pair of even integers is even. □

(b) **There exist positive integers a, b and c such that $a^2 + b^2 = c^2$.**

Proof. Consider the positive integers $a = 3$, $b = 4$, $c = 5$. Then $a^2 + b^2 = 9 + 16 = 25 = c^2$. □

(c) **There is an even integer n such that $5n - 4$ is prime.** This statement is **false**. We prove the negation: $\forall n \in \mathbb{Z}^{\text{even}}$, $5n - 4$ is not prime.

Proof. Suppose that n is an even integer. Thus $n = 2k$ for some integer k. Hence

$$5n - 4 = 5(2k) - 4 = 10k - 4 = 2(5k - 2).$$

By definition, this means that $5n - 4$ is even. The only even prime is 2. If $2(5k - 2) = 2$, then $5k - 2 = 1$ and hence $k = \frac{3}{5}$ which is not an integer. Therefore $5n - 4$ is not a prime number. □

(d) **$\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.**

Proof. Suppose n is a positive integer and $n \geq 4$. Let us factor

$$2n^2 - 5n + 2 = (2n - 1)(n - 2).$$

Since $n \geq 4$, we have $2n - 1 \geq 7$ and $n - 2 \geq 2$, so both factors are integers > 1. Hence the expression is composite for all $n \geq 4$. □

(e) **$\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.** This statement is **false**. Take $x = 1$ and $y = -2$. Then $y^2 = 4 > x^2 = 1$, but $y = -2 \not> 1 = x$.

2. Take $x = \frac{3}{2}$. Then $\lfloor x^2 \rfloor = \lfloor \frac{9}{4} \rfloor = 2$, while $\lfloor x \rfloor^2 = \lfloor \frac{3}{2} \rfloor^2 = 1^2 = 1$. Hence $\lfloor x^2 \rfloor \neq \lfloor x \rfloor^2$, so the statement is false.

3. (a) **Statement.** The difference between any odd integer and any even integer is odd.

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. **[Error: using k for both m and n means that the statement is only proved when $m = n + 1$.]** Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

Correct proof. Let m be any odd integer and let n be any even integer. Then there exist $k, \ell \in \mathbb{Z}$ such that $m = 2k + 1$ and $n = 2\ell$. Hence

$$m - n = (2k + 1) - 2\ell = 2(k - \ell) + 1,$$

which is an odd integer by definition. □

(b) **Statement.** If a and b are even integers, then $4a + 2b$ is even. **[Error: the proof forgets to state its assumptions.]**

Proof. We have $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Then we want to show that $4a + 2b$ is even, so

$$\begin{aligned} 4a + 2b &= 2\ell \quad \textbf{[Error: this line assumes what is to be proved.]} \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

therefore the statement is true.

Correct proof. Suppose a and b are even integers. Then $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Therefore

$$4a + 2b = 4(2k) + 2(2j) = 8k + 4j = 2(4k + 2j).$$

Since $k, j \in \mathbb{Z}$, we have $(4k + 2j) \in \mathbb{Z}$ and so, by definition, $4a + 2b$ is even. □

(c) **Statement.** $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $xy = 1$.

Proof. This is true, for example if $x = 10$ then let $y = \frac{1}{10}$ and $xy = 10 \cdot \frac{1}{10} = 1$. Therefore the statement is true. **[Error: the proof argues from a single example, which cannot establish a universal statement. Moreover, the statement is false.]**

Correct disproof. The statement is false. As a counterexample, let $x = 0$. We know that $0 \cdot y = 0$ for all $y \in \mathbb{R}$ and so there is no real number y such that $0 \cdot y = 1$. □

(d) **Statement.** $\forall n \in \mathbb{Z}$, if $n > 0$ then $n^2 + 2n + 1$ is composite.

Proof. Suppose n is an integer and $n > 0$, then we want to show that n^2+2n+1 is composite, so this means

$n^2+2n+1 = rs$ **[Error: forgets to define r, s — e.g. for some $r, s \in \mathbb{Z}$]**

where

$$1 < r, s < n^2 + 2n + 1$$

Clearly neither r nor s are equal to 1 so $n^2 + 2n + 1$ is not prime and hence must be composite. **[Error: this is jumping to the conclusion without showing what needs to be shown. The expression we need to show (the definition of composite) has been given but it has not been shown.]**

Correct proof. Let $n \in \mathbb{Z}$ with $n > 0$. Then we have

$$n^2 + 2n + 1 = (n + 1)(n + 1).$$

Now since $0 < n < n^2 + 2n$, we must have that $1 < n + 1 < n^2 + 2n + 1$. So by letting $r = s = n + 1$ we have shown that

$$n^2 + 2n + 1 = rs$$

for integers $1 < r, s < n^2 + 2n + 1$. By definition this means $n^2 + 2n + 1$ is composite. □

Application — Applications of Proofs to Computer Science

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 74–80.*

Computer programs have been developed to automate the task of reasoning and proving theorems. Many of these programs make use of a rule of inference known as **resolution**. This rule of inference is based on the tautology

$$((p \vee q) \wedge (\sim p \vee r)) \rightarrow (q \vee r) \tag{1}$$

Resolution can be used to build automatic theorem proving systems.

To construct proofs using resolution as the only rule of inference, the hypotheses and conclusion must be expressed as **clauses**. Clauses are logical expressions which only feature disjunctions of variables or their negations (i.e. expressions which only use $\vee$, $\sim$, so they do not use $\wedge$, $\rightarrow$). To express any statement as a clause, we can use the laws of logical equivalence.

Application problems

1. (a) Using a truth table, show that expression (1) is a tautology.

   (b) Write the following expressions as clauses.

   i. $\sim (\sim r \wedge w)$

   ii. $r \rightarrow u$

   iii. $\sim (u \wedge w)$

   (c) Use resolution only to show that the following argument is valid:

   If it is raining, then Yvette has their umbrella. It is not the case that Yvette has their umbrella and gets wet. It is not the case that Yvette gets wet while it is not raining. Therefore, Yvette does not get wet.

Application solutions

1. (a) The truth table is

p	q	r	$p \vee q$	$\sim p \vee r$	$(p \vee q) \wedge (\sim p \vee r)$	$q \vee r$	$((p \vee q) \wedge (\sim p \vee r)) \rightarrow (q \vee r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	T	T
T	F	T	T	T	T	T	T
T	F	F	T	F	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	F	T	F	T	T
F	F	F	F	T	F	F	T

Since the last column is always T, the statement is a tautology.

(b) Clause forms:

i. $\sim (\sim r \wedge w) \equiv r \vee \sim w$ (by De Morgan's law and double negative law).

ii. $r \rightarrow u \equiv \sim r \vee u$ (by definition of implication).

iii. $\sim (u \wedge w) \equiv \sim u \vee \sim w$ (by De Morgan's law).

(c) Define the following variables:

r	it is raining
u	Yvette has their umbrella
w	Yvette gets wet

Then we can express the argument as

1. $r \rightarrow u$
2. $\sim (u \wedge w)$
3. $\sim (\sim r \wedge w) \therefore \sim w$

Using the equivalences in (b), we can rewrite this as

1.	$\sim r \vee u$	
2.	$\sim u \vee \sim w$	
3.	$r \vee \sim w$	
4.	$\sim r \vee \sim w$	From 1 and 2 by Resolution
5.	$\sim w$	From 3 and 4 by Resolution.

§10 — Proof by Contradiction

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 8 (week 3). Notes: proof-techniques[362]*.*

Problems

1. Prove the following statement using a proof by contradiction:

   For integers a and b, if $6a + 3b$ is odd, then b is odd.

2. Use a proof by contradiction to prove the following statement:

   For all positive integers x and y, $x^2 - y^2 \neq 1$.

Solutions

1. **For integers a and b, if $6a + 3b$ is odd, then b is odd.**

   Proof. Suppose the statement is false, that is, suppose that there exist integers a and b for which $6a + 3b$ is odd and b is even.

   Since b is even, $b = 2k$ for some integer k. Thus

   $$6a + 3b = 6a + 3(2k) = 6a + 6k = 2(3a + 3k).$$

   Since $a, k \in \mathbb{Z}$, $3a + 3k \in \mathbb{Z}$ so $6a + 3b$ is even. This contradicts our assumption that $6a + 3b$ is odd, so our assumption was incorrect and hence the original statement is true. □

[362] courses/math1061/proof-techniques.pdf

2. **For all positive integers x and y, $x^2 - y^2 \neq 1$.**

   Proof. Suppose, for contradiction, that x and y are positive integers satisfying $x^2 - y^2 = 1$. Now, by factoring, we have

   $$1 = x^2 - y^2 = (x - y)(x + y).$$

   Since x and y are positive integers, we must have $x - y = 1$ and $x + y = 1$. This means $2x = 2$, so $x = 1$. But then we must have $y = 0$ which is not a positive integer; this is a contradiction. Therefore the original statement is true. □

§11 — Proof by Contraposition

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 9 (week 3). Notes: proof-techniques[363].

Problems

1. Use proof by contraposition to prove the following statement:

   For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.

2. Prove the following statement:

   For any integer n, n^2 is odd if and only if n is odd.

   Use a direct proof for the reverse implication ($\Leftarrow$), and a proof by contraposition for the forward implication ($\Rightarrow$).

3. Use proof by contraposition to prove the following statement:

   For all integers x and y, if $x^2(y^2 - 2y)$ is odd then x and y are odd.

[363] courses/math1061/proof-techniques.pdf

Solutions

1. **For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.**

   Proof. We prove the contrapositive statement, which is:

   > For all integers a and b, if a is even or b is even, then $(ab)^2$ is even.

   Let a and b be integers and suppose a is even or b is even. Without loss of generality, suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $ab = 2kb$ is even, and therefore $(ab)^2 = 4k^2b^2 = 2(2k^2b^2)$. Since $k, b \in \mathbb{Z}$, we know $2k^2b^2 \in \mathbb{Z}$, so $(ab)^2$ is even by definition. □

2. **For any integer n, n^2 is odd if and only if n is odd.**

   Proof. To prove this "if and only if" statement, we must prove each of the following two statements:

   > ($\Leftarrow$) For any integer n, if n is odd, then n^2 is odd. ($\Rightarrow$) For any integer n, if n^2 is odd, then n is odd.

   ($\Leftarrow$) Let n be an integer and suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. Hence $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$. Since $k \in \mathbb{Z}$, we have $2k^2+2k \in \mathbb{Z}$ and hence n^2 is odd by definition.

   ($\Rightarrow$) The contrapositive is: for any integer n, if n is even, then n^2 is even. Let n be an integer and suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$. Hence $n^2 = 4k^2 = 2(2k^2)$. Since $k \in \mathbb{Z}$, we have $2k^2 \in \mathbb{Z}$, so n^2 is even by definition.

   Therefore, for all integers n, n^2 is odd if and only if n is odd. □

3. **For all integers x and y, if $x^2(y^2-2y)$ is odd then x and y are odd.**

   Proof. We will prove the contrapositive statement, which is:

   > For all integers x and y, if x is even or y is even, then $x^2(y^2-2y)$ is even.

   Let $x, y \in \mathbb{Z}$ and suppose x or y is even. We consider the cases of x even or y even individually.

   Case 1. Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Hence

   $$x^2(y^2-2y) = (2k)^2(y^2-2y) = 2(2k^2)(y^2-2y).$$

   Since $k, y \in \mathbb{Z}$, we have $(2k^2)(y^2-2y) \in \mathbb{Z}$, and hence $x^2(y^2-2y)$ is even, by definition.

Case 2. Suppose y is even. Then $y = 2\ell$ for some $\ell \in \mathbb{Z}$. Hence

$$x^2(y^2 - 2y) = x^2((2\ell)^2 - 2(2\ell)) = 2(x^2(2\ell^2 - 2\ell)).$$

Since $x, \ell \in \mathbb{Z}$, we have $x^2(2\ell^2 - 2\ell) \in \mathbb{Z}$ and thus $x^2(y^2 - 2y)$ is even, by definition. □

§12 — Rational Numbers

Epp 4th ed. pp. 163–170 · 5th ed. (metric) pp. 183–190. Lecture 9 (week 3). Notes: rational-and-irrational-numbers[364].

Problems

1. Prove the following statement:

   For real numbers m and n, if m is irrational and n is rational, then $m - n$ is irrational.

2. Prove the following statement:

   For a real number r, if $2r^2 - 3r$ is irrational, then r is irrational.

3. Prove the following statement:

   For all real numbers r, s, n, if r is irrational, s is rational and n is a positive integer, then $n(r-s)$ is irrati

4. Recall that $\sqrt{2}$ is irrational. Consider the statement

   For every rational number r, if $r \neq 0$, then $r\sqrt{2}$ is an irrational number.

   (a) Write down the negation of the statement.

   (b) Use a proof by contradiction to prove the statement.

[364] courses/math1061/rational-and-irrational-numbers.pdf

Solutions

1. **For real numbers m and n, if m is irrational and n is rational, then $m-n$ is irrational.**

   Proof. Let m and n be real numbers and suppose (for a contradiction) that m is an irrational number and n is rational, but $m-n$ is rational. Since n is rational, we have $n=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. Since $m-n$ is rational, we have $m-n=\frac{c}{d}$ for some $c,d\in\mathbb{Z}$ where $d\neq 0$.

   Notice that $m=(m-n)+n$. Hence

   $$m=(m-n)+n=\frac{c}{d}+\frac{a}{b}=\frac{bc+ad}{bd}.$$

   Since $a,b,c,d\in\mathbb{Z}$ we have $bc+ad\in\mathbb{Z}$ and $bd\in\mathbb{Z}$. Further, since $b\neq 0$ and $d\neq 0$, we have $bd\neq 0$. Thus, by definition, m is rational. But this contradicts the assumption that m is irrational. □

2. **For a real number r, if $2r^2-3r$ is irrational, then r is irrational.**

   Proof. We prove the contrapositive statement: for a real number r, if r is rational, then $2r^2-3r$ is rational.

   Let r be a real number and suppose $r\in\mathbb{Q}$. Then $r=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. So

   $$2r^2-3r=2\left(\frac{a}{b}\right)^2-3\left(\frac{a}{b}\right)=\frac{2a^2-3ab}{b^2}.$$

   Since $a,b\in\mathbb{Z}$, we have $2a^2-3ab\in\mathbb{Z}$ and $b^2\in\mathbb{Z}$. Further, $b^2\neq 0$ because $b\neq 0$. This means $2r^2-3r$ is rational, by definition. □

3. **For all real numbers r, s, and n, if r is irrational, s is rational and n is a positive integer, then $n(r-s)$ is irrational.**

   Proof. Suppose, for a contradiction, that the statement is false. Then there exist real numbers r, s and n such that r is an irrational number, s is rational, n is a positive integer, but $n(r-s)$ is rational. Since s is rational, $s=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. Since $n(r-s)$ is rational, we have $n(r-s)=\frac{c}{d}$ for some $c,d\in\mathbb{Z}$ where $d\neq 0$.

Now,

$$\begin{aligned} r - s &= n(r-s)\left(\frac{1}{n}\right) \quad \text{noting that } n \neq 0 \\ r - s &= \frac{c}{d} \cdot \frac{1}{n} \\ r &= s + \frac{c}{d} \cdot \frac{1}{n} \\ &= \frac{a}{b} + \frac{c}{dn} \\ &= \frac{adn + bc}{bdn} \end{aligned}$$

Since $a, b, c, d \in \mathbb{Z}$, we have $adn + bc \in \mathbb{Z}$ and $bdn \in \mathbb{Z}$. Further, since $b \neq 0$, $d \neq 0$ and $n \neq 0$, we have $bdn \neq 0$. This means r is rational, by definition, which is a contradiction. □

4. **For every rational number r, if $r \neq 0$, then $r\sqrt{2}$ is an irrational number.**

   (a) **Negation:** There exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$.

   (b)

   Proof. Suppose, for a contradiction, that the original statement is false. Then there exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$. Since r is rational, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and since $r \neq 0$, we have $a \neq 0$. Since we have assumed $r\sqrt{2}$ is rational, $r\sqrt{2} = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

   Now

$$\sqrt{2} = \frac{r\sqrt{2}}{r} = \left(r\sqrt{2}\right)\left(\frac{1}{r}\right) = \frac{c}{d} \cdot \frac{b}{a} = \frac{bc}{ad}.$$

   Since $a, b, c, d \in \mathbb{Z}$, we know $bc \in \mathbb{Z}$ and $ad \in \mathbb{Z}$. Further, since $a \neq 0$ and $d \neq 0$, we have $ad \neq 0$. Thus, by definition, $\sqrt{2}$ is rational. However, this is a contradiction, as $\sqrt{2}$ is irrational. Thus, the original statement is true. □

§13 — Divisibility

Epp 4th ed. pp. 170–179 · 5th ed. (metric) pp. 190–199. Lecture 10 (week 4). Notes: divisibility-and-factorisation[365].

[365] courses/math1061/divisibility-and-factorisation.pdf

Problems

1. Find the unique factorisation (in standard form) of the integer 27 720.
2. Prove or disprove the statement: for any integers m, n, and q, if $m \mid n$ and $n \mid q$ then $m^2 \mid nq$.
3. Prove the following statements.
   (a) If k is any even integer and m is any odd integer, then $(k+2)^2-(m-3)^2$ is divisible by 4.
   (b) The difference between the cube of two consecutive integers leaves the remainder 1 when it is divided by 6.
4. Use proof by contradiction to prove this statement:

$$\text{For all integers } c, d \text{ and } e, \text{ if } c \mid d \text{ and } c \nmid e, \text{ then } c \nmid (d+e).$$

Solutions

1. By repeated division, we have $27\,720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.
2. **For any integers m, n, and q, if $m \mid n$ and $n \mid q$ then $m^2 \mid nq$.** The statement is **true**, and we will prove it.

   Proof. Let m, n, and q be non-zero integers. Assume $m \mid n$ and $n \mid q$. Then, by definition, there exist integers a, b such that

   $$n = ma \quad \text{and} \quad q = nb.$$

   Then observe

   $$nq = (ma)(nb) = ma \cdot (mab) = m^2(a^2b).$$

   Since $a^2b \in \mathbb{Z}$, we conclude that $m^2 \mid nq$. □
3. (a) **If k is any even integer and m is any odd integer, then $(k+2)^2-(m-3)^2$ is divisible by 4.**

   Proof. Let k be even and m be odd. Then $k = 2a$ and $m = 2b+1$ for some $a, b \in \mathbb{Z}$. Hence

   $$(k+2)^2 = (2a+2)^2 = 4(a+1)^2 \quad \text{and} \quad (m-3)^2 = (2b-2)^2 = 4(b-1)^2.$$

   Therefore

   $$(k+2)^2-(m-3)^2 = 4\big[(a+1)^2-(b-1)^2\big].$$

   Since $a, b \in \mathbb{Z}$ we have $(a+1)^2-(b-1)^2 \in \mathbb{Z}$ so $4 \mid \big[(k+2)^2-(m-3)^2\big]$. □

(b) **The difference between the cube of two consecutive integers leaves the remainder 1 when it is divided by 6.**

Proof. Let n and $n+1$ be two consecutive integers. The difference between their cubes is

$$(n+1)^3 - n^3 = 3n^2 + 3n + 1 = 3n(n+1) + 1.$$

Now whether n is odd or even (so whatever integer n is), one of n, $n+1$ will be odd and the other one will be even. Thus the product $n(n+1)$ is even.

Since $n(n+1)$ is even, write $n(n+1) = 2t$ for some $t \in \mathbb{Z}$. Then

$$(n+1)^3 - n^3 = 3(2t) + 1 = 6t + 1 \equiv 1 \pmod 6.$$

Hence the remainder is 1 upon division by 6. □

4. **For all integers c, d and e, if $c \mid d$ and $c \nmid e$, then $c \nmid (d+e)$.**

Proof. Suppose for a contradiction that the statement is false. Then there exist integers c, d and e such that $c \mid d$ and $c \nmid e$ and $c \mid (d+e)$.

Now $c \mid d$ means that $d = cx$ for some integer x. And $c \mid (d+e)$ means that $d + e = cy$ for some integer y.

Hence $d + e = cx + e = cy$, so $e = cy - cx = c(y - x)$, and we have $y - x \in \mathbb{Z}$, because x and y are both integers. Thus $c \mid e$, a contradiction. So the original statement is true. □

§14 — Modular Arithmetic

Epp 4th ed. pp. 482–485 · 5th ed. (metric) pp. 528–531. Lecture 11 (week 4). Notes: modular-arithmetic[366].

Problems

1. Prove the following statement:

   If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.

2. (a) Evaluate $58 \operatorname{div} 11$ and $58 \bmod 11$.

[366] courses/math1061/modular-arithmetic.pdf

(b) Find integers q and r, with $0 \leqslant r < d$ and $n = dq + r$, in the case that $n = -95$ and $d = 11$.

3. (a) An integer n, when divided by 7, leaves remainder 4. What is the remainder (between 0 and 6 inclusive) when $3n$ is divided by 7?

   (b) When the integer m is divided by 11, the remainder 9 is left. What remainder is left when $4m$ is divided by 22?

4. Prove or disprove the following statements.

   (a) For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.

   (b) For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.

Solutions

1. **If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.**

   Proof. Fix $y \in \mathbb{Z}$. By the division algorithm, $y = 5m + r$ for some $m \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3, 4\}$. Then

   $$y^2 = (5m + r)^2 = 25m^2 + 10mr + r^2 \equiv r^2 \pmod 5.$$

   Let us compute the possible values for r^2 mod 5:

   $$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 4, \quad 4^2 \equiv 16 \equiv 1 \pmod 5.$$

   Thus $y^2 \equiv 0, 1$, or $4 \pmod 5$, and never 2 or 3. □

2. (a) Since $58 = 11 \cdot 5 + 3$ with $0 \leq 3 < 11$, we have

   $$58 \operatorname{div} 11 = 5 \quad \text{and} \quad 58 \bmod 11 = 3.$$

   (b) We want $-95 = 11q + r$ with $0 \leq r < 11$. Taking $q = -9$ gives

   $$11(-9) = -99 \quad \Rightarrow \quad -95 = -99 + 4 = 11(-9) + 4,$$

   so $q = -9$ and $r = 4$.

3. (a) If n leaves remainder 4 upon division by 7, then $n = 7k + 4$ for some integer k. Hence

$$3n = 21k + 12 = 7(3k + 1) + 5,$$

so the remainder when $3n$ is divided by 7 is **5**. (The source PDF prints this step as $7(3k) + 5$, which equals $21k + 5$, not $21k + 12$ — the quotient is $3k + 1$, as above. The answer of 5 is unaffected.)

(b) If m leaves remainder 9 upon division by 11, then $m = 11k + 9$ for some integer k. Then

$$4m = 44k + 36 = 22(2k + 1) + 14,$$

so the remainder when $4m$ is divided by 22 is **14**.

4. (a) **For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** The statement is **false**. For a counterexample, take $x = \frac{3}{2}$. Then

$$\lfloor x^2 \rfloor = \left\lfloor \frac{9}{4} \right\rfloor = 2 \quad \text{but} \quad \lfloor x \rfloor^2 = \left\lfloor \frac{3}{2} \right\rfloor^2 = 1^2 = 1.$$

(b) **For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.** The statement is **true**.

Proof. Let n be an odd integer, so $n = 2k + 1$ for some integer k. Then

$$\frac{n^2}{4} = \frac{(2k+1)^2}{4} = \frac{4k^2 + 4k + 1}{4} = k(k+1) + \frac{1}{4},$$

so $\left\lfloor \frac{n^2}{4} \right\rfloor = k(k+1)$. Moreover, notice

$$\left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right) = \left(\frac{2k}{2}\right)\left(\frac{2k+2}{2}\right) = k(k+1).$$

Hence $\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)$ for all odd integers n. □

§15 — The Euclidean Algorithm

Epp 4th ed. pp. 220–224 · 5th ed. (metric) pp. 250–254. Lecture 12 (week 4). Notes: gcd-lcm-and-euclidean-algorithm[367].

[367] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

Problems

1. Use the Euclidean Algorithm to determine $\gcd(14, 3003)$.
2. Compute
   (a) $\operatorname{lcm}(12, 18)$
   (b) $\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2)$
   (c) $\operatorname{lcm}(2800, 6125)$
3. Prove that for all positive integers a and b, we have

$$\gcd(a, b) = \operatorname{lcm}(a, b) \iff a = b.$$

4. Prove that for all positive integers a and b, we have

$$a \mid b \iff \operatorname{lcm}(a, b) = b.$$

5. (a) Use the Euclidean algorithm to determine $\gcd(931, 301)$. Show your working.
   (b) Write down the unique prime factorisation of 931 in standard form.
   (c) How many positive divisors does 931 have? (Hint: use part (b).)
6. (a) Using the Euclidean algorithm, compute $\gcd(116, 88)$. Show your working.
   (b) Using your answer to part (a), compute $\operatorname{lcm}(116, 88)$.

Solutions

1. We apply the Euclidean Algorithm:

$$3003 = 14 \cdot 214 + 7, \qquad 14 = 7 \cdot 2 + 0.$$

   Hence $\gcd(14, 3003) = 7$.

2. (a) We factor $12 = 2^2 \cdot 3$ and $18 = 2 \cdot 3^2$ so $\operatorname{lcm}(12, 18) = 2^2 \cdot 3^2 = 36$.
   (b) Using the maximum exponents of each prime, we have

$$\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2) = 2^3 \cdot 3^2 \cdot 5 = 360.$$

   (c) We factor $2800 = 2^4 \cdot 5^2 \cdot 7$ and $6125 = 5^3 \cdot 7^2$. Thus

$$\operatorname{lcm}(2800, 6125) = 2^4 \cdot 5^3 \cdot 7^2 = 98000.$$

3. **For all positive integers a and b, $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$.**

   Proof. Let a and b be positive integers.

   ($\Longleftarrow$) It is clear that if $a = b$ then $\gcd(a, b) = \operatorname{lcm}(a, b)$.

   ($\Longrightarrow$) Assume $\gcd(a, b) = \operatorname{lcm}(a, b)$. Denoting $g = \gcd(a, b)$, we have $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$.

   Now notice gm and gn have no common prime factors beyond those in g, so the least common multiple uses all primes from both m and n. Therefore

   $$\operatorname{lcm}(a, b) = gmn.$$

   Now, we have $g = gmn$. Therefore $mn = 1$, and so $m = n = 1$. This lets us conclude $a = b$. □

4. **For all positive integers a and b, $a \mid b$ if and only if $\operatorname{lcm}(a, b) = b$.**

   Proof. Let us denote $g = \gcd(a, b)$ so that $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$. As explained in the previous question, we have

   $$\operatorname{lcm}(a, b) = gmn.$$

   ($\Longrightarrow$) If $a \mid b$, then $gm \mid gn$, hence $m \mid n$. Since $\gcd(m, n) = 1$, we conclude $m = 1$. Therefore $\operatorname{lcm}(a, b) = gmn = gn = b$.

   ($\Longleftarrow$) If $\operatorname{lcm}(a, b) = b$, then $gmn = gn$ which means $m = 1$. Therefore $a = gm = g$ and so $a \mid b$. □

5. (a) Using the Euclidean Algorithm:

   $$\begin{aligned} 931 &= 301 \cdot 3 + 28 \\ 301 &= 28 \cdot 10 + 21 \\ 28 &= 21 \cdot 1 + 7 \\ 21 &= 7 \cdot 3 + 0. \end{aligned}$$

   Hence $\gcd(931, 301) = 7$.

   (b) Since $\gcd(931, 301) = 7$, we know $7 \mid 931$, and we have $931 = 7 \cdot 133$. The number 133 has prime factorisation $7 \cdot 19$. Therefore the unique prime factorisation of 931 is $7^2 \cdot 19$.

(c) We have $931 = 7^2 \cdot 19^1$ from part (b). Any divisor of 931 must have a prime factorisation of the form $7^a \cdot 19^b$ where $a \in \{0, 1, 2\}$ and $b \in \{0, 1\}$. Thus the number of positive divisors is

$$(2 + 1)(1 + 1) = 6.$$

(There are 3 choices for the exponent a and 2 choices for the exponent b.)

6. (a) Using the Euclidean Algorithm:

$$\begin{aligned} 116 &= 88 \cdot 1 + 28 \\ 88 &= 28 \cdot 3 + 4 \\ 28 &= 4 \cdot 7 + 0 \end{aligned}$$

Hence $\gcd(116, 88) = 4$.

(b) Using $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ for $a, b \in \mathbb{Z}^+$,

$$\operatorname{lcm}(116, 88) = \frac{116 \cdot 88}{\gcd(116, 88)} = \frac{116 \cdot 88}{4} = 116 \cdot 22 = 2552.$$

Application — Trace Tables for Algorithms

Not assessable for MATH1061. For reference, see S. Epp, Discrete Mathematics with Applications, *Section 4.8 (4th edition) or Section 4.10 (5th edition), Brooks/Cole, Belmont, CA.*

The following pseudo-code describes the **Division Algorithm**, with annotations to explain what each step is doing.

Input: a (a non-negative integer), d (a positive integer). This algorithm will take two inputs, a and d, and will find the quotient $a \operatorname{div} d$ and the remainder $a \bmod d$.

Algorithm body:

```
r := a          -- defining our variables
q := 0
                -- starting with a, repeatedly subtract lots of d until we reach
                -- a number less than d; each round adds 1 to the quotient count
while r >= d,
    r := r - d
    q := q + 1
end while
```

Output: q, r. Once we have obtained a number less than d, we are finished. The output q is the quotient ($a \operatorname{div} d$) and the output r is the remainder ($a \bmod d$).

The following pseudo-code describes the **Euclidean Algorithm**, with annotations to explain what each step is doing.

Input: A, B (integers with $A > B \geq 0$).

Algorithm body:

```
a := A          -- defining our variables
b := B
r := B
                -- if b /= 0, compute a mod b (call the algorithm above for this
                -- step) and set r to be this value; replace a with b and b with r
                -- and repeat until b = 0
while b /= 0,
    r := a mod b
    a := b
    b := r
end while
gcd := a
```

Output: gcd (a positive integer).

A **trace table** keeps track of the value of each variable at each step of an algorithm. For example, the trace table for the Division Algorithm with input variables $a = 19$ and $d = 4$ is:

Variable / iteration	0	1	2	3	4
a	19				
d	4				
r	19	15	11	7	3
q	0	1	2	3	4

Output: $q = 4$, $r = 3$.

Application problems

1. Construct a trace table to trace the action of the Division Algorithm for the following inputs.

   (i) $a = 26$, $d = 7$

(ii) $a = 15$, $d = 6$

2. Construct a trace table to trace the action of the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$.

Application solutions

1. (i) Trace table for the Division Algorithm with $a = 26$, $d = 7$:

Variable / iteration	0	1	2	3
a	26			
d	7			
r	26	19	12	5
q	0	1	2	3

Output: $q = 3$, $r = 5$.

(ii) Trace table for the Division Algorithm with $a = 15$, $d = 6$:

Variable / iteration	0	1	2
a	15		
d	6		
r	15	9	3
q	0	1	2

Output: $q = 2$, $r = 3$.

2. Trace table for the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$:

Variable / iteration	0	1	2	3	4	5
A	1001					
B	871					
a	1001	871	130	91	39	13
b	871	130	91	39	13	0
r	871	130	91	39	13	0
gcd						13

Output: gcd = 13.

§16 — Sequences

Epp 4th ed. pp. 227–244 · 5th ed. (metric) pp. 258–275. Lecture 13 (week 5).

Problems

1. Write down the first four terms in the sequence defined by $a_k = \dfrac{k}{10+k}$ for $k = 1, 2, \ldots$.
2. Consider the sequences $a_k = 2k + 1$ and $b_k = (k-1)^3 + k + 2$ where $k = 0, 1, 2, \ldots$. Show that the first three terms of these sequences are identical, but that their fourth terms differ.
3. (a) Find an explicit formula for a sequence c_n whose first six terms are $-1, 1, -1, 1, -1, 1$.
   (b) Find an explicit formula for a sequence d_n whose first six terms are $\frac{1}{4}, \frac{2}{9}, \frac{3}{16}, \frac{4}{25}, \frac{5}{36}, \frac{6}{49}$.
4. (a) Write $(x^2-1)+(2x^3-1)+(3x^4-1)+(4x^5-1)+(5x^6-1)$ in summation notation.
   (b) Evaluate $\displaystyle\prod_{i=1}^{5}(-1)^i \cdot i$.
   (c) Write $(y-1)(y^2-2)(y^3-3)(y^4-4)$ in product notation.
   (d) Evaluate $\displaystyle\sum_{j=1}^{n}(-1)^j\frac{1}{2^j}$ when $n = 5$.

Solutions

1. We have

$$a_1 = \frac{1}{11}, \qquad a_2 = \frac{2}{12} = \frac{1}{6}, \qquad a_3 = \frac{3}{13}, \qquad a_4 = \frac{4}{14} = \frac{2}{7}.$$

2. We compute

$$a_0 = 1, \quad a_1 = 3, \quad a_2 = 5, \quad a_3 = 7;$$

$$b_0 = (-1)^3+0+2 = 1, \quad b_1 = 0^3+1+2 = 3, \quad b_2 = 1^3+2+2 = 5, \quad b_3 = 2^3+3+2 = 13.$$

Hence the first three terms agree ($a_0 = b_0$, $a_1 = b_1$ and $a_2 = b_2$), but the fourth terms differ ($a_3 = 7$ while $b_3 = 13$).

3. (a) One explicit formula is

$$c_n = (-1)^n \qquad n = 1, 2, 3, ...$$

(b) The denominators are square numbers, so an explicit formula is

$$d_n = \frac{n}{(n+1)^2} \qquad n = 1, 2, 3, ...$$

4. (a) We have

$$(x^2 - 1) + (2x^3 - 1) + (3x^4 - 1) + (4x^5 - 1) + (5x^6 - 1) = \sum_{k=1}^{5} \left(kx^{k+1} - 1\right).$$

(b) We have

$$\prod_{i=1}^{5} (-1)^i \cdot i = \left(\prod_{i=1}^{5} (-1)^i\right) \left(\prod_{i=1}^{5} i\right) = (-1)^{1+2+3+4+5} \cdot 5! = (-1)^{15} \cdot 120 = -120.$$

(c) We have

$$(y-1)(y^2-2)(y^3-3)(y^4-4) = \prod_{k=1}^{4} \left(y^k - k\right).$$

(d) When $n = 5$, we have

$$\sum_{j=1}^{5} (-1)^j \frac{1}{2^j} = -\frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \frac{1}{16} - \frac{1}{32} = -\frac{11}{32}.$$

§17 — Mathematical Induction

Epp 4th ed. pp. 244–268 · 5th ed. (metric) pp. 275–301. Lecture 13 (week 5).

Problems

1. Use mathematical induction to prove the following statements.

   (a) For every positive integer n, $n(n+1)$ is even.

   (b) For every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.

   (c) For all integers $n \geq 7$, $3^n < n!$.

   (d) For each integer $n \geq 1$,

   $$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

   (e) For each integer $n \geq 0$, $1 + 4n \leq 5^n$.

Solutions

1. (a) **For every positive integer n, $n(n+1)$ is even.**

   Proof. Let $P(n)$ be the predicate "$n(n+1)$ is even".

   Basis: when $n = 1$, $n(n+1) = 2$ which is even, so $P(1)$ is true.

   (The inductive step is to show that for all integers $k \geq 1$, $P(k)$ implies $P(k+1)$.)

   Inductive hypothesis: suppose that for some integer $k \geq 1$, $P(k)$ is true. Thus $k(k+1) = 2a$ for some integer a.

   Now consider $n = k + 1$. Then

   $$(k+1)(k+2) = k(k+1) + 2(k+1) = 2a + 2(k+1) = 2(a+k+1).$$

   Since a and k are integers, $a + k + 1$ is an integer, so $(k+1)(k+2)$ is even and $P(k+1)$ is true.

   Thus, by the principle of mathematical induction, $n(n+1)$ is even for every positive integer n. □

   (b) **For every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.**

Proof. Let $P(n)$ be the predicate $6 \mid (n^3 - n)$.

Basis: when $n = 2$, $n^3 - n = 8 - 2 = 6$. Since $6 \mid 6$, $P(2)$ is true.

(The inductive step is to show that for all integers $k \geq 2$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose that for some integer $k \geq 2$, $P(k)$ is true. Thus $k^3 - k = 6a$ for some integer a.

Now consider $n = k + 1$. Then

$$(k+1)^3-(k+1) = k^3+3k^2+3k+1-k-1 = k^3-k+3k^2+3k = 6a+3k(k+1).$$

For the integer k, $k(k+1)$ is even from part (a), so let $k(k+1) = 2b$ for some integer b. Hence $(k+1)^3 - (k+1) = 6a + 3(2b) = 6(a+b)$. Thus $6 \mid ((k+1)^3 - (k+1))$ and so $P(k+1)$ is true.

Thus, by the principle of mathematical induction, $n^3 - n$ is a multiple of 6 for each integer $n \geq 2$. □

(c) **For all integers $n \geq 7$, $3^n < n!$.**

Proof. Let $P(n)$ be the predicate $3^n < n!$.

Basis: $P(7)$ is the statement $3^7 < 7!$. The left-hand side is $3^7 = 2187$ and the right-hand side is $7! = 5040$, so $P(7)$ holds.

(The inductive step is to show that for all integers $k \geq 7$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: let $k \geq 7$ be an integer and assume that $P(k)$ is true; that is $3^k < k!$. We will now show that $P(k+1)$ holds, so we will show $3^{k+1} < (k+1)!$.

Taking the right-hand side, we have

$$\begin{aligned}
(k+1)! &= (k+1) \cdot k! \\
&> (k+1) \cdot 3^k && \text{by the inductive hypothesis} \\
&> 3 \cdot 3^k && \text{since } k \geq 7 \\
&= 3^{k+1}
\end{aligned}$$

Hence $P(k+1)$ is true.

Thus by the principle of mathematical induction, for all integers $n \geq 7$, $3^n < n!$. □

(d) **For each integer $n \geq 1$, $\displaystyle\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.**

Proof. Let $P(n)$ be the predicate

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

Basis: consider $n = 1$. We have $\sum_{i=1}^{1} i^3 = 1^3 = 1$ and $\frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$ so $P(1)$ is true.

(The inductive step is to show that for all integers $k \geq 1$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(k)$ is true. That is,

$$\sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4}.$$

Now consider $n = k + 1$.

$$\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 && \text{(splitting off the last term)} \\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3 && \text{by the inductive hypothesis} \\
&= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\
&= \frac{(k+1)^2}{4}(k^2 + 4(k+1)) \\
&= \frac{(k+1)^2}{4}(k^2 + 4k + 4) \\
&= \frac{(k+1)^2}{4}(k+2)^2
\end{aligned}$$

Thus $P(k+1)$ is true.

Therefore, by the principle of mathematical induction, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$ for every integer $n \geq 1$. □

(e) **For each integer $n \geq 0$, $1 + 4n \leq 5^n$.**

Proof. Let $P(n)$ be the predicate $1 + 4n \leq 5^n$.

Basis: when $n = 0$ we have $1 + 4 \cdot 0 \leq 5^0$, so $P(0)$ is true.

(The inductive step is to show that for all integers $k \geq 0$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose $k \geq 0$ is an integer and $P(k)$ is true; that is, $1 + 4k \leq 5^k$.

Now consider $n = k + 1$. Starting with the left-hand side of $P(k+1)$, we have

$$\begin{aligned} 1 + 4(k+1) &= 1 + 4k + 4 \\ &\leq 5^k + 4 && \text{by the inductive hypothesis} \\ &\leq 5^k + 4 \cdot 5^k && \text{since } k \geq 0 \text{ so } 5^k \geq 1 \\ &= 5(5^k) \\ &= 5^{k+1} \end{aligned}$$

so $P(k+1)$ is true.

Thus, by the principle of mathematical induction, $1 + 4n \leq 5^n$ for every integer $n \geq 0$. □

§18 — Strong Induction and the Well Ordering Principle

Epp 4th ed. pp. 268–279 · 5th ed. (metric) pp. 301–314. Lecture 14 (week 5).

Problems

1. Consider the statement

   For every integer $n \geq 2$, there exist integers $a, b \geq 0$ such that $n = 2a + 3b$.

   (a) Prove the statement using the well-ordering principle.

   (b) Prove the statement using strong mathematical induction.

2. The Lucas sequence $a_1, a_2, a_3, ...$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. Use strong mathematical induction to prove that $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{Z}^+$.

3. Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Use strong mathematical induction to prove $a_n := x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.

Solutions

1. **For every integer $n \geq 2$, there exist integers $a, b \geq 0$ such that $n = 2a + 3b$.**

   (a)

Proof (using the well-ordering principle). Consider the set of counterexamples

$$S = \{\, n \in \mathbb{Z}^{\geq 2} : \text{there do not exist integers } a, b \geq 0 \text{ with } n = 2a + 3b \,\}.$$

If S is empty, we are done. Otherwise, by the well-ordering principle, S has a least element. Let us call it N.

Notice that $2 \notin S$ because $2 = 2 \cdot 1 + 3 \cdot 0$, and $3 \notin S$ because $3 = 2 \cdot 0 + 3 \cdot 1$. Also $4 \notin S$ because $4 = 2 \cdot 2 + 3 \cdot 0$. Hence $N \geq 5$. By minimality of N, we must have $N - 2 \notin S$. Therefore there exist integers $a, b \geq 0$ such that

$$N - 2 = 2a + 3b.$$

In other words, we have

$$N = 2(a + 1) + 3b.$$

This means $N \notin S$, contradicting the assumption that $N \in S$. Hence S is empty, and the statement holds for all $n \geq 2$. $\square$

(b)

Proof (using strong induction). Let $P(n)$ be the predicate: "there exist integers $a, b \geq 0$ such that $n = 2a + 3b$."

Basis: we have

$$2 = 2 \cdot 1 + 3 \cdot 0, \qquad 3 = 2 \cdot 0 + 3 \cdot 1, \qquad 4 = 2 \cdot 2 + 3 \cdot 0,$$

so $P(2)$, $P(3)$, $P(4)$ are true.

(The inductive step is to show that for every integer $k \geq 4$, if $P(2), P(3), \ldots, P(k)$ are all true then $P(k + 1)$ is true.)

Inductive hypothesis: suppose $k \geq 4$ is an integer and assume $P(m)$ is true for every integer $m = 2, 3, \ldots, k$.

Consider $n = k + 1$. Since $k \geq 4$, we have $k - 1 \geq 3$, so by the inductive hypothesis $P(k - 1)$ is true. Thus there exist $a, b \geq 0$ such that

$$k - 1 = 2a + 3b.$$

Adding 2 gives

$$k + 1 = 2(a + 1) + 3b,$$

so $P(k + 1)$ holds. $\square$

2. **The Lucas sequence** $a_1, a_2, a_3, \ldots$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. Prove that $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{Z}^+$.

Proof. Let $P(n)$ be the predicate $a_n \leqslant \left(\frac{7}{4}\right)^n$.

Basis: when $n = 1$, $a_1 = 1 \leqslant \left(\frac{7}{4}\right)^1 = 1\frac{3}{4}$ is true, so $P(1)$ is true. When $n = 2$, $P(2)$ holds because $a_2 = 3 \leqslant \left(\frac{7}{4}\right)^2 = \frac{49}{16} = 3\frac{1}{16}$.

(The inductive step is to show that for every integer $k \geq 1$, if $P(1), \ldots, P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and that $P(m)$ is true for all m with $1 \leq m \leq k$.

Now consider $P(k+1)$, which we want to prove holds. We have

$$\begin{aligned}
a_{k+1} &= a_k + a_{k-1} \\
&\leqslant \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} && \text{by the inductive hypothesis} \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4} + 1\right) \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{11}{4}\right) \\
&\leqslant \left(\frac{7}{4}\right)^{k-1}\left(\frac{49}{16}\right) && \text{noting } \tfrac{11}{4} = \tfrac{44}{16} < \tfrac{49}{16} \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2 \\
&= \left(\frac{7}{4}\right)^{k+1}.
\end{aligned}$$

Hence $P(k+1)$ holds. Therefore, by the principle of strong mathematical induction, $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all integers $n \geqslant 1$. □

3. **Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Prove $a_n := x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.**

Proof. Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Let $P(n)$ be the predicate "a_n is an integer."

Basis: $P(0)$ holds since $a_0 = x^0 + \frac{1}{x^0} = 2$. $P(1)$ holds since $a_1 = x + \frac{1}{x}$, which is an integer by assumption.

(The inductive step is to show that for every integer $k \geq 1$, if $P(0), P(1), \ldots, P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(m)$ holds for all integers $m = 0, 1, \ldots, k$.

We now aim to show that $P(k+1)$ is true. Notice that

$$\begin{aligned} a_1 a_k &= \left(x + \frac{1}{x}\right)\left(x^k + \frac{1}{x^k}\right) \\ &= \left(x^{k+1} + \frac{1}{x^{k+1}}\right) + \left(x^{k-1} + \frac{1}{x^{k-1}}\right) = a_{k+1} + a_{k-1}. \end{aligned}$$

Therefore $a_{k+1} = a_1 a_k - a_{k-1}$. By the inductive hypothesis, a_k and a_{k-1} are integers, and a_1 is an integer, so a_{k+1} is an integer. Hence $P(k+1)$ holds.

Therefore, by the principle of strong mathematical induction, a_n is an integer for all $n \geq 0$. □

§19 — Recursive Definitions

Epp 4th ed. pp. 290–304 · 5th ed. (metric) pp. 325–340. Lecture 15 (week 6).

Problems

1. Define the sequence $b_1 = 2$, $b_2 = 6$ and

$$b_k = b_{k-1} + b_{k-2} + \gcd(b_{k-1}, b_{k-2})$$

for all $k \geq 3$. Use strong induction to prove b_n is even for all $n \geq 1$.

2. A sequence is defined by $a_1 = 2$ and

$$a_k = k(a_{k-1} + k - 1)$$

for all integers $k \geq 2$. Use mathematical induction to prove a_n is even for all $n \geq 1$.

3. Recursively define the set S of binary strings as follows.

   (a) *(Base rule)* $1 \in S$.

   (b) *(Recursion rule)* If $s \in S$ then $0s \in S$ and $1s \in S$ (e.g. if $s = 1$ then $0s = 01$).

   (c) *(Restriction rule)* No other strings lie in S besides those given by the rules above.

   What are the strings contained in S arising from the first three applications of the recursive rule?

Solutions

1. *Proof.* Let $P(n)$ be the predicate "b_n is even".

   Base case. The base cases are $n = 1, 2$. We have $b_1 = 2$ and $b_2 = 6$ so $P(1)$ and $P(2)$ are true.

   Inductive hypothesis. Assume $P(m)$ is true for all integers m with $1 \leq m \leq k$, where $k \geq 2$ is an integer. That is, we assume $b_1, b_2, \ldots, b_k$ are all even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. b_{k+1} is even. Using the recursive definition, we have

   $$b_{k+1} = b_k + b_{k-1} + \gcd(b_k, b_{k-1}).$$

   By the inductive hypothesis, b_k and b_{k-1} are even, so $2 \mid b_k$ and $2 \mid b_{k-1}$, hence $2 \mid \gcd(b_k, b_{k-1})$ as well. Therefore each term on the right-hand side is even, so their sum b_{k+1} is even. Thus $P(k+1)$ holds.

   Therefore, b_n is even for all integers $n \geq 1$. □

2. *Proof.* Let $P(n)$ be the predicate "a_n is even".

   Base case. The base case is $n = 1$. We have $a_1 = 2$, which is even, so $P(1)$ is true.

   Inductive hypothesis. Assume $P(k)$ is true for some integer $k \geq 1$. That is, assume a_k is even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. a_{k+1} is even. By the recursive definition, we have

   $$a_{k+1} = (k+1)(a_k + (k+1) - 1) = (k+1)(a_k + k).$$

   Note that a_k is even by the inductive hypothesis. We split into cases:

   - If k is even, then $a_k + k$ is even, hence a_{k+1} is even.
   - If k is odd, then $k+1$ is even, hence a_{k+1} is even.

   In all cases, a_{k+1} is even, so $P(k+1)$ is true.

   Therefore, a_n is even for all integers $n \geq 1$. □

3. By the base rule, we only know $1 \in S$.

   First application of the recursive rule:

   $$01 \in S, \qquad 11 \in S.$$

   Second application of the recursive rule:

$$001 \in S, \quad 101 \in S, \quad 011 \in S, \quad 111 \in S.$$

Third application of the recursive rule:

$$0001 \in S, \quad 1001 \in S, \quad 0101 \in S, \quad 1101 \in S,$$
$$0011 \in S, \quad 1011 \in S, \quad 0111 \in S, \quad 1111 \in S.$$

§20 — Solving Recurrence Relations

Epp 4th ed. pp. 304–328 · 5th ed. (metric) pp. 340–364. Lecture 16 (week 6).

Problems

1. Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that

$$a_n = 5a_{n-1} - 6a_{n-2}$$

for all integers $n \geq 2$.

2. Let $\{b_n\}_{n\geq 0}$ be the sequence defined by

$$b_0 = 2, \qquad b_1 = 5, \qquad \text{and} \qquad b_k = 2b_{k-1} - b_{k-2} \text{ for each integer } k \geq 2.$$

   (a) Write down the values of $b_0, b_1, b_2, b_3, b_4, b_5$.

   (b) Based on your answers for part (a), guess an explicit formula for this sequence.

   (c) Prove that your guess from part (b) is correct.

3. Let T_n be a sequence defined by $T_1 = 1$ and

$$T_{n+1} = 1 + (T_1 \times T_2 \times T_3 \times \cdots \times T_n)$$

for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.

4. Consider the Fibonacci sequence defined recursively by

$$\begin{aligned} a_0 &= 0 \\ a_1 &= 1 \\ a_n &= a_{n-2} + a_{n-1} \qquad \text{for all integers } n \geq 2. \end{aligned}$$

Use strong mathematical induction to prove the explicit formula

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}$$

for all integers $n \geq 0$, where $\phi = \frac{1+\sqrt{5}}{2}$ and $\psi = \frac{1-\sqrt{5}}{2}$. (You may use the fact that $\phi^2 = \phi + 1$ and $\psi^2 = \psi + 1$.)

Solutions

1. **Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$.**

Proof. For $n \geq 2$, we have $n - 2 \geq 0$ so all three terms a_n, a_{n-1} and a_{n-2} are defined in the given formula. Then,

$$\begin{aligned} 5a_{n-1} - 6a_{n-2} &= 5\left(2^{n-1} + 5 \cdot 3^{n-1}\right) - 6\left(2^{n-2} + 5 \cdot 3^{n-2}\right) \\ &= \left(5 \cdot 2^{n-1} - 6 \cdot 2^{n-2}\right) + \left(25 \cdot 3^{n-1} - 30 \cdot 3^{n-2}\right) \\ &= (10 - 6)2^{n-2} + (75 - 30)3^{n-2} \\ &= 4 \cdot 2^{n-2} + 45 \cdot 3^{n-2} \\ &= 2^n + 5 \cdot 3^n \\ &= a_n. \end{aligned}$$

Hence $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$. □

2. (a)

$$\begin{aligned} b_0 &= 2 \\ b_1 &= 5 \\ b_2 &= 2(5) - 2 = 8 \\ b_3 &= 2(8) - 5 = 11 \\ b_4 &= 2(11) - 8 = 14 \\ b_5 &= 2(14) - 11 = 17 \end{aligned}$$

(b) Guess that $b_n = 3n + 2$ for each integer $n \geq 0$.

(c)

Proof. The guess gives $b_0 = 3(0) + 2 = 2$ and $b_1 = 3(1) + 2 = 5$ so it gives the correct initial conditions. Now we substitute the guess into the recurrence relation. The LHS of the recurrence relation is $b_k = 3k + 2$. The RHS of the recurrence relation is

$$\begin{aligned} 2b_{k-1} - b_{k-2} &= 2(3(k-1)+2) - (3(k-2)+2) \\ &= 2(3k-1) - (3k-4) \\ &= 6k - 2 - 3k + 4 \\ &= 3k + 2 \end{aligned}$$

So the guess also satisfies the recurrence relation. Thus the guess is correct. □

Alternative proof (by strong induction). Let $P(n)$ be the predicate $b_n = 3n + 2$.

Basis: $b_0 = 2$ from the recursive definition and $3(0) + 2 = 2$ so $P(0)$ is true. $b_1 = 5$ from the recursive definition and $3(1) + 2 = 5$ so $P(1)$ is true.

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(0), P(1), \ldots, P(k)$ are true.

Now

$$\begin{aligned} b_{k+1} &= 2b_k - b_{k-1} && \text{by the rec. rel. since } k+1 \geq 2 \\ &= 2(3k+2) - (3(k-1)+2) && \text{since } P(k) \text{ and } P(k-1) \text{ are true} \\ &= 6k + 4 - (3k - 1) \\ &= 3k + 5 \\ &= 3(k+1) + 2 \end{aligned}$$

So $P(k+1)$ is true. Therefore, by the principle of (strong) mathematical induction, the guess is correct for this recursively defined sequence. □

3. **Let T_n be a sequence defined by $T_1 = 1$ and $T_{n+1} = 1 + (T_1 \times \cdots \times T_n)$ for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.**

Proof. We can prove this simply by applying the recursive formula twice, once for T_{n+1} and once for T_n:

$$\begin{aligned} T_{n+1} &= 1 + (T_1 \cdot T_2 \cdot T_3 \cdots T_n) && \text{by the recursive definition} \\ &= 1 + T_n \cdot (T_1 \cdot T_2 \cdot T_3 \cdots T_{n-1}) \\ &= 1 + T_n \cdot (T_n - 1) && \text{since } T_n = 1 + (T_1 \cdots T_{n-1}) \text{ by rec. def.} \\ &= 1 + (T_n)^2 - T_n \\ &= (T_n)^2 - T_n + 1. \end{aligned}$$

Note that both applications of the recursive definition are valid, since $n-1 \geq 1$. $\square$

4. **Fibonacci explicit formula.**

Proof. Let $P(n)$ be the predicate

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}.$$

Basis. The base cases are $n = 0, 1$, which are true because

$$\frac{\phi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0 = a_0,$$

and

$$\frac{\phi - \psi}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = a_1.$$

Inductive hypothesis. Now suppose that for some integer $m \geq 1$, we have that $P(i)$ is true for all $0 \leq i \leq m$. In particular, $P(m)$ and $P(m-1)$ are true, that is,

$$a_m = \frac{\phi^m - \psi^m}{\sqrt{5}} \qquad \text{and} \qquad a_{m-1} = \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}}.$$

We need to show that $P(m+1)$ is true. That is, we aim to show

$$a_{m+1} = \frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}}.$$

Starting with the right-hand side of $P(m+1)$, we have

$$\begin{aligned}
\frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}} &= \frac{\phi^2\phi^{m-1} - \psi^2\psi^{m-1}}{\sqrt{5}} \\
&= \frac{(\phi+1)\phi^{m-1} - (\psi+1)\psi^{m-1}}{\sqrt{5}} && \text{since } \phi^2 = \phi + 1 \text{ and } \psi^2 = \psi + 1 \\
&= \frac{(\phi^m + \phi^{m-1}) - (\psi^m + \psi^{m-1})}{\sqrt{5}} \\
&= \frac{\phi^m - \psi^m}{\sqrt{5}} + \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}} \\
&= a_m + a_{m-1} && \text{by the inductive hypothesis} \\
&= a_{m+1} && \text{by definition.}
\end{aligned}$$

Hence $P(m+1)$ is true. $\square$

§21 — Set Theory Definitions

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Define the sets

$$\begin{aligned} V &= \{x \in \mathbb{Z} \mid 2 \leqslant x \leqslant 11 \text{ and } x \text{ is odd}\}, \\ X &= \{x \in \mathbb{Z} \mid -1 \leqslant x \leqslant 4\}, \\ Y &= \{2, 3, 7, 9\}, \\ Z &= \{x \in \mathbb{Z} \mid x \neq 0\}. \end{aligned}$$

   Write down the following sets, listing their elements and using brackets as appropriate.

   (a) $V \cap X$. (b) $V \cup Y$. (c) $X \cap Z$.

   (b) $X \cap (Z - Y)$. (e) $(X \cup Y) \cap V$. (f) $X \cup (Y \cap V)$.

2. For each of the following sets, write down its elements and then state the size of the set; that is, find $|A|$, $|B|$, $|C|$ and $|D|$.

   (a) $A = \{x \in \mathbb{Z} \mid \exists\, i \in \mathbb{Z} \text{ such that } x = 1 + (-1)^i\}$.

   (b) $B = \{y \in \mathbb{Z} \mid -8 < y \leqslant -5\}$.

   (c) $C = \{s \in \mathbb{Z} \mid s^2 + 1 = 0\}$.

   (d) $D = \{t \in \mathbb{Z} \mid t^4 = 1\}$.

3. Define the sets $A = \{0, 1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$ and $C = \{1, 2, 4, 5, 7\}$. List the elements of the set

$$R = ((A - B) \cap (A - C)) \cup (B \cap C \cap A).$$

4. Are the following statements true or false? Justify in one or two sentences.

   (a) $x \in \{x\}$ (b) $\{x\} \subseteq \{x\}$ (c) $\{\emptyset\} \in \{\{\emptyset\}\}$

   (b) $\emptyset \subseteq \{x\}$ (e) $\emptyset \in \{x\}$

Solutions

1. (a) $V \cap X = \{3\}$

   (b) $V \cup Y = \{2, 3, 5, 7, 9, 11\}$

   (c) $X \cap Z = \{-1, 1, 2, 3, 4\}$

   (d) $X \cap (Z - Y) = \{-1, 1, 4\}$

   (e) $(X \cup Y) \cap V = \{3, 7, 9\}$

   (f) $X \cup (Y \cap V) = \{-1, 0, 1, 2, 3, 4, 7, 9\}$

2. (a) Note that $(-1)^i$ is either $+1$ or -1 (according as i is even or odd). So x is either $1 + 1$ or $1 - 1$, that is, 2 or 0. So $A = \{2, 0\}$ and $|A| = 2$.

   (b) $B = \{-7, -6, -5\}$, so $|B| = 3$.

   (c) If $s^2 + 1 = 0$, we have $s^2 = -1$, and there are no such real numbers s, let alone integers! So $C = \emptyset$ and $|C| = 0$.

   (d) $D = \{-1, 1\}$, since $t^4 = 1$ with $t \in \mathbb{Z}$ implies $t = \pm 1$. Hence $|D| = 2$.

3. We have $A - B = \{0, 1, 2\}$ and $A - C = \{0, 3\}$, so $(A - B) \cap (A - C) = \{0\}$. Also $B \cap C \cap A = \{4\}$. Thus $R = \{0\} \cup \{4\} = \{0, 4\}$.

4. (a) **True:** $\{x\}$ is the set whose only element is x, so $x \in \{x\}$.

   (b) **True:** every set is a subset of itself, so $\{x\} \subseteq \{x\}$.

   (c) **True:** $\{\{\emptyset\}\}$ has the single element $\{\emptyset\}$, so $\{\emptyset\} \in \{\{\emptyset\}\}$.

   (d) **True:** $\emptyset \subseteq S$ for every set S, in particular $\emptyset \subseteq \{x\}$.

   (e) **False** (in general): $\emptyset \in \{x\}$ would require $\emptyset = x$.

Application — Computer Representations of Sets

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 134–138.*

There are various ways to represent sets using a computer. One such method involves the use of binary strings.

If we fix a finite universal set U with an arbitrary ordering, for example $U = \{a_1, a_2, \ldots, a_n\}$, we can represent subsets of U using binary strings of length n. A 1 in the ith position of the string indicates that element a_i is in the subset and a 0 indicates it is not.

For example if $U = \{1, 2, 3\}$ then the string 000 represents the empty set, 101 represents the subset $\{1, 3\}$ and 111 represents the entire set U.

The set operations union and intersection can be computed at the level of binary strings by utilising the bitwise OR and AND operations. The union of two sets corresponds to the bitwise OR operation on the strings and the intersection corresponds to bitwise AND.

Application problems

1. Define the universal set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

   (a) Express each of the following subsets of U using binary strings:

   i. $\{3, 4, 5\}$

   ii. $\{1, 3, 6, 10\}$

   iii. $\{a \in U \mid a \text{ is prime}\}$.

   (b) Using the same U, find the set represented by the following strings:

   i. 1111001111

   ii. 0101111000

   iii. 1000000001

   (c) Use binary strings to compute the following set operations.

   i. $\{1, 3, 4, 6, 10\} \cap \{2, 3, 6, 9, 10\}$

   ii. $\{2, 4, 6, 8\} \cup \{3, 4, 5\}$

Application solutions

1. (a) i. 0011100000

   ii. 1010010001

   iii. 0110101000 — the primes in U are $2, 3, 5, 7$. (The source PDF prints 1010111000 here, which decodes to $\{1, 3, 5, 6, 7\}$ and is not the set of primes; the string above is the correct one.)

   (b) i. $\{1, 2, 3, 4, 7, 8, 9, 10\}$

   ii. $\{2, 4, 5, 6, 7\}$

   iii. $\{1, 10\}$

   (c) i. 1011010001 AND 0110010011 = 0010010001, so the intersection is $\{3, 6, 10\}$.

   ii. 0101010100 OR 0011100000 = 0111110100, so the union is $\{2, 3, 4, 5, 6, 8\}$.

§22 — More Definitions and Examples of Sets

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Let $A = \{1, 2\}$, $B = \{2, 3\}$ and $C = \{3, 4\}$. List the elements of the following sets.
   (a) $A \cap C$
   (b) $(A \cup C) - B$
   (c) $(A \times B) \cap (A \times C)$
   (d) $\mathcal{P}(B \cap C)$
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\}$
2. Are the following statements true or false?
   (a) $\mathbb{Q} \in \mathbb{R}$.
   (b) $\{1, 2\} \subseteq \mathbb{Z}$.
   (c) $\{-3, 0\} \subseteq \mathcal{P}(\mathbb{Z})$.
   (d) $\{(1, 2), (0, 1)\} \in \mathbb{Z} \times \mathbb{Z}$.
3. Let $X = \mathcal{P}(\emptyset)$ and $Y = \mathcal{P}(\mathcal{P}(\emptyset))$. List the elements of each of the following sets.
   (a) X (b) Y (c) $X \cap Y$ (d) $X \cup Y$
4. Define sets $S = \{3, 5\}$ and $T = \{2, 3, 7\}$. Are the following statements true or false?
   (a) $S \subseteq T$
   (b) $\emptyset \in \mathcal{P}(S)$
   (c) $\emptyset \in T$
   (d) $(3, 3, 3) \in S \times T$

Solutions

1. (a) $A \cap C = \emptyset$.
   (b) $(A \cup C) - B = \{1, 4\}$.
   (c) $(A \times B) \cap (A \times C) = \{(1, 3), (2, 3)\}$.
   (d) $\mathcal{P}(B \cap C) = \{\emptyset, \{3\}\}$.
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\} = \{\emptyset, \{2\}\}$.
2. (a) **False.** ($\mathbb{Q}$ is a *subset* of $\mathbb{R}$, not an element of it.)
   (b) **True.**
   (c) **False.** (The elements of $\mathcal{P}(\mathbb{Z})$ are sets of integers; -3 and 0 are integers, not sets.)
   (d) **False.** (It is a *subset* of $\mathbb{Z} \times \mathbb{Z}$, not an element — the elements of $\mathbb{Z} \times \mathbb{Z}$ are ordered pairs.)
3. (a) $X = \mathcal{P}(\emptyset) = \{\emptyset\}$.
   (b) $Y = \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.
   (c) $X \cap Y = \{\emptyset\}$.
   (d) $X \cup Y = \{\emptyset, \{\emptyset\}\}$.
4. (a) **False.** ($5 \in S$ but $5 \notin T$.)
   (b) **True.** (The empty set is an element of every power set.)
   (c) **False.** (T's elements are 2, 3 and 7.)
   (d) **False.** (The elements of $S \times T$ are ordered *pairs*, not triples.)

§23 — Properties of Sets

Epp 4th ed. pp. 352–366 · 5th ed. (metric) pp. 391–407. Lecture 18 (week 7).

Problems

1. (a) Use the element method to prove that for all sets A and B

$$A \cup (B - A) = A \cup B.$$

   (b) Use the element method to prove that for all sets X, Y and Z,

$$(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset.$$

   (c) Use set identities to prove that for all sets A, B and C

$$(A - B) - C = A - (B \cup C).$$

2. Prove or disprove the following:

   (a) For all sets A and B, we have $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

   (b) For all sets A and B, we have $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$.

   (c) There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.

   (d) Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$.

3. Let A, B and C be sets. Prove that

$$A - (B \cup C) = (A - B) - C.$$

Solutions

1. (a) **For all sets A and B, $A \cup (B - A) = A \cup B$.**

   Proof. First we show that $A \cup (B - A) \subseteq A \cup B$.

   Consider an arbitrary element $x \in A \cup (B - A)$. Then we know $x \in A$ or $x \in B - A$. This means $x \in A$, or $x \in B$ and $x \notin A$. If $x \in A$, then $x \in A \cup B$. Similarly if $x \in B - A$, then it must be in B and so $x \in A \cup B$. In either case, we have $x \in A \cup B$, thus $A \cup (B - A) \subseteq A \cup B$.

   Now we show that $A \cup B \subseteq A \cup (B - A)$.

   Let $x \in A \cup B$, then $x \in A$ or $x \in B$ or it is in both A and B. If $x \in A$, then $x \in A \cup (B - A)$. If $x \notin A$ then $x \in B$ since $x \in A \cup B$. So we have that $x \in B$ and $x \notin A$, hence $x \in B - A$ and thus $x \in A \cup (B - A)$. This proves that $A \cup B \subseteq A \cup (B - A)$, and together this proves that $A \cup B = A \cup (B - A)$. $\square$

(b) **For all sets X, Y and Z, $(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset$.**

Proof. Assume that $(X - Z) \cap (Y - Z) \cap (X - Y) \neq \emptyset$.

So let $x \in (X - Z) \cap (Y - Z) \cap (X - Y)$. Then, in particular, $x \in Y - Z$ and $x \in X - Y$. The former implies $x \in Y$, but the latter implies $x \notin Y$. No such x exists. Therefore the set is empty. □

(c) **For all sets A, B and C, $(A - B) - C = A - (B \cup C)$.**

Proof. Using $A - B = A \cap B^c$, $(S - T) = S \cap T^c$, and De Morgan's law, we have

$$(A-B)-C = (A\cap B^c)\cap C^c = A\cap(B^c\cap C^c) = A\cap(B\cup C)^c = A-(B\cup C). \qquad \square$$

2. (a) **For all sets A and B, $\mathcal{P}(A\cup B) = \mathcal{P}(A)\cup\mathcal{P}(B)$. False.** Counterexample: $A = \{1\}$, $B = \{2\}$. Then

$$\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \neq \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\} = \{\emptyset, \{1\}, \{2\}\}.$$

(b) **For all sets A and B, $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$. True.**

($\Longleftarrow$) If $A = B$ then clearly $\mathcal{P}(A) = \mathcal{P}(B)$.

($\Longrightarrow$) We next show that if $\mathcal{P}(A) = \mathcal{P}(B)$, then $A = B$. Suppose (for a contradiction) that $\mathcal{P}(A) = \mathcal{P}(B)$ but $A \neq B$. Then (without loss of generality), there exists an element x in A that is not in B. Therefore, there is an element $\{x\}$ in $\mathcal{P}(A)$ that is not in $\mathcal{P}(B)$. Therefore $\mathcal{P}(A) \neq \mathcal{P}(B)$ — a contradiction. Thus, for all sets A and B, if $\mathcal{P}(A) = \mathcal{P}(B)$ then $A = B$. □

(c) **There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$. False.**

No such set exists. The power set of any set must contain the empty set — that is, $\emptyset \in \mathcal{P}(A)$, where A is any set. Also, the power set of any set of size n has cardinality 2^n. The power set above contains 7 elements, and there does not exist any integer n such that $2^n = 7$.

(d) **Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$. True.**

First note that if $A = \emptyset$ then $A \times B = A \times C = \emptyset$ and the statement is true. Also, if $B = \emptyset$ then $A \times B = \emptyset$ and $\emptyset \subseteq A \times C$ for any C, so the statement is true.

Suppose A, B and C are non-empty sets with $B \subseteq C$. Thus if $b \in B$, then $b \in C$. Consider any element $(a, b) \in A \times B$, where $a \in A$ and $b \in B$. Since

$b \in B$, $b \in C$. As such, $a \in A$ and $b \in C$ for all a or b, so $(a, b) \in A \times C$. Therefore $A \times B \subseteq A \times C$. □

3. **For all sets A, B and C, $A - (B \cup C) = (A - B) - C$.**

   Proof Option 1. For any x, we have

   $$x \in A - (B \cup C) \iff x \in A \wedge x \notin (B \cup C) \iff x \in A \wedge (x \notin B) \wedge (x \notin C).$$

   Also, we have

   $$x \in (A - B) - C \iff x \in (A - B) \wedge x \notin C \iff (x \in A \wedge x \notin B) \wedge x \notin C.$$

   The statements on the right-hand side are equivalent. Hence $A - (B \cup C) = (A - B) - C$. □

   Proof Option 2.

   $$\begin{aligned} A - (B \cup C) &= A \cap (B \cup C)^c && \text{by the Set Difference Law} \\ &= A \cap (B^c \cap C^c) && \text{by De Morgan's law} \\ &= (A \cap B^c) \cap C^c && \text{by Associative law} \\ &= (A - B) \cap C^c && \text{by the Set Difference Law} \\ &= (A - B) - C && \text{by the Set Difference Law} \quad \square \end{aligned}$$

§24 — Functions Defined on General Sets

Epp 4th ed. pp. 383–396 · 5th ed. (metric) pp. 425–439. Lecture 18 (week 7).

Problems

1. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 - 1$.
   (a) What is the domain, codomain and range of f?
   (b) What is the image of $\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}$ under f?
   (c) What is the preimage of $\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}$ under f?
2. Let $X = \{1, 3, 5\}$ and $Y = \{s, t, u, v\}$ be sets. Define $f : X \to Y$ by the arrow diagram

   $$1 \mapsto v, \qquad 3 \mapsto s, \qquad 5 \mapsto v$$

   (the elements t and u of Y receive no arrows).

(a) Write the domain of f and the co-domain of f.

(b) Determine $f(1)$, $f(3)$, and $f(5)$.

(c) Determine the range of f.

(d) Is 3 an inverse image of s? Is 1 an inverse image of u?

(e) What is the inverse image of s? of u? of v?

(f) Represent f as a set of ordered pairs.

3. Let D be the set of all finite subsets of $\mathbb{Z}^+$. Consider the function $T : \mathbb{Z}^+ \to D$ defined by $T(n) := \{d \mid d \in \mathbb{Z}^+ \text{ and } d \text{ divides } n\}$. Find the following:

(a) $T(1)$ (b) $T(15)$ (c) $T(17)$ (d) $T(5)$ (e) $T(18)$ (f) $T(21)$

4. Let S be the set of all strings of a's and b's.

(a) Define the function $f : S \to \mathbb{Z}$ by

$$f(s) = \begin{cases} \text{the number of } b\text{'s to the left of the left-most } a \text{ in } s, & \text{if } s \text{ contains an } a, \\ 0, & \text{if } s \text{ contains no } a\text{'s.} \end{cases}$$

Find $f(aba)$, $f(bbab)$, and $f(b)$. What is the range of f?

(b) Define the function $g : S \to S$ by

$$g(s) = \text{the string obtained by writing the characters of } s \text{ in reverse order.}$$

Find $g(aba)$, $g(bbab)$, and $g(b)$. What is the range of g?

Solutions

1. (a) The domain is $\mathbb{R}$, the codomain is $\mathbb{R}$, and the range is $[-1, \infty)$.

(b) $f(\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}) = [-1, 3]$.

(c) $f^{-1}(\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}) = \{x \in \mathbb{R} \mid 1 \leq x^2 \leq 4\} = [-2, -1] \cup [1, 2]$.

2. (a) The domain is $X = \{1, 3, 5\}$ and the codomain is $Y = \{s, t, u, v\}$.

(b) $f(1) = v$, $f(3) = s$, $f(5) = v$.

(c) $\text{range}(f) = \{s, v\}$.

(d) **Yes**, 3 is an inverse image of s. **No**, 1 is not an inverse image of u.

(e) $f^{-1}(s) = \{3\}$, $f^{-1}(u) = \emptyset$, $f^{-1}(v) = \{1, 5\}$.

(f) $f = \{(1, v), (3, s), (5, v)\}$.

3. (a) $T(1) = \{1\}$.

(b) $T(15) = \{1, 3, 5, 15\}$.

(c) $T(17) = \{1, 17\}$.

(d) $T(5) = \{1, 5\}$.

(e) $T(18) = \{1, 2, 3, 6, 9, 18\}$.

(f) $T(21) = \{1, 3, 7, 21\}$.

4. (a) $f(aba) = 0$, $f(bbab) = 2$, $f(b) = 0$, $\text{range}(f) = \mathbb{Z}^{\geq 0}$.

(b) $g(aba) = aba$, $g(bbab) = babb$, $g(b) = b$, $\text{range}(g) = S$.

§25 — one-to-one, Onto, and Inverse Functions

Epp 4th ed. pp. 397–416 · 5th ed. (metric) pp. 439–461. Lecture 19 (week 7).

Problems

1. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = \left\lfloor \dfrac{1 - 6n}{3} \right\rfloor$.

(a) Is f one-to-one?

(b) Is f onto?

(c) Is f bijective?

(d) Prove or disprove that for all $m, n \in \mathbb{Z}$, we have $f(mn) = f(m)f(n)$.

2. Define the set $A = \{0, 1, 2, 3, 4\}$ and the functions $f : A \to A$ and $g : A \to A$ by

$$f(a) = (a + 4)^2 \pmod 5, \qquad g(a) = (a^2 + 3a + 1) \pmod 5.$$

Is $f = g$?

3. Consider the function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f((m, n)) = 2^m 3^n$.

(a) Determine $f((3, 1))$.

(b) Determine the pre-image of $\{36\}$.

(c) Prove f is one-to-one.

4. Consider the function $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x^2 \rfloor$.

   (a) What is the image $f([-1, 1])$?

   (b) What is the preimage $f^{-1}(\{1\})$?

   (c) Is f one-to-one?

   (d) Is f onto?

   (e) Is f bijective?

Solutions

1. First, we note that, for $n \in \mathbb{Z}$,

$$f(n) = \left\lfloor \frac{1-6n}{3} \right\rfloor = \left\lfloor -2n + \frac{1}{3} \right\rfloor = -2n$$

   since $-2n \in \mathbb{Z}$ and $\frac{1}{3} \in [0, 1)$.

   (a) **Yes.** If $f(m) = f(n)$ then $-2m = -2n$, hence $m = n$. Therefore f is one-to-one.

   (b) **No.** Since $f(n) = -2n$ we see that f never maps to any odd integer; for example, there is no integer w with $f(w) = 1$. Therefore f is not onto.

   (c) **No**, f is not a bijection. (It is injective but not surjective.)

   (d) This is **false**; take $m = n = 1$. Then $f(mn) = -2$ but $f(m)f(n) = 4$.

2. **Yes.** First note f and g have the same domain and codomain. This means we just need to show $f(a) = g(a)$ for all $a \in A$. Notice that we have

$$(a+4)^2 = a^2 + 8a + 16 \equiv a^2 + 3a + 1 \pmod 5,$$

   so $f(a) = g(a)$ for all $a \in A$, and hence $f = g$.

3. (a) $f((3, 1)) = 2^3 3^1 = 24$.

   (b) $36 = 2^2 3^2$, so $f((m, n)) = 36$ if and only if $(m, n) = (2, 2)$. Hence $f^{-1}(\{36\}) = \{(2, 2)\}$.

   (c) If $f((m, n)) = f((m', n'))$, then $2^m 3^n = 2^{m'} 3^{n'}$, so $2^{m-m'} = 3^{n'-n}$. By unique prime factorisation, this forces $m - m' = 0$ and $n' - n = 0$. That is, $m = m'$ and $n = n'$, and hence $(m, n) = (m', n')$. So f is one-to-one.

4. (a) Note that if $x \in [-1, 1]$ then $x^2 \in [0, 1]$. This means we have $\lfloor x^2 \rfloor \in \{0, 1\}$. Both values occur because $\lfloor 0^2 \rfloor = 0$ and $\lfloor 1^2 \rfloor = 1$. Thus $f([-1, 1]) = \{0, 1\}$.

(b) $f^{-1}(\{1\}) = \{x \in \mathbb{R} : 1 \leq x^2 < 2\} = (-\sqrt{2}, -1] \cup [1, \sqrt{2})$.

(c) **No**, f is not one-to-one. For example, $f\left(\frac{1}{2}\right) = 0 = f\left(-\frac{1}{2}\right)$ but $\frac{1}{2} \neq -\frac{1}{2}$.

(d) **No**, f is not onto since $f(x) = \lfloor x^2 \rfloor \geq 0$ for all x. This means, for instance, that -1 is not in the image of f.

(e) **No**, f is not bijective.

§26 — Composition of Functions

Epp 4th ed. pp. 416–427 · 5th ed. (metric) pp. 461–472. Lecture 20 (week 7).

Problems

1. Let $f, g : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^3 - 1$ and $g(x) = x + 5$.

   (a) Determine the functions $(g \circ f)(x)$ and $(f \circ g)(x)$.

   (b) Is $g \circ f$ a bijection?

2. Define $f : \mathbb{Q} \to \mathbb{Z}$ by $f(x) = 2\lfloor x + 1 \rfloor$.

   (a) What is the range of f?

   (b) Is f one-to-one?

   (c) Is f onto?

   (d) Define $g : \mathbb{Z} \to \mathbb{Z}$ by $g(x) = 2x - 1$. Determine the composition $(g \circ f)(x)$.

   (e) Calculate $(g \circ f)\left(-\frac{3}{4}\right)$.

   (f) What is the range of $g \circ f$?

3. Let f and g be functions. Prove or disprove the following statements:

   (a) If f and $f \circ g$ are one-to-one, then g is one-to-one.

   (b) If f and $f \circ g$ are onto, then g is onto.

Solutions

1. (a) We have

$$(g \circ f)(x) = g(x^3 - 1) = x^3 + 4$$

and

$$(f \circ g)(x) = f(x + 5) = (x + 5)^3 - 1 = x^3 + 15x^2 + 75x + 124.$$

(b) **No**, $g \circ f$ is not a bijection. The map $x \mapsto x^3 + 4$ is one-to-one on $\mathbb{Z}$, but it is not onto (e.g. 0 is not in its image since $x^3 = -4$ has no integer solution).

2. (a) The range is a subset of the even integers because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. If $2m$ is an even integer then $f(m - 1) = 2\lfloor m - 1 + 1 \rfloor = 2m$, so the range is the set of all even integers.

(b) **No**, f is not one-to-one. For example,

$$f(0) = 2\lfloor 0 + 1 \rfloor = 2\lfloor 1 \rfloor = 2 \times 1 = 2, \quad \text{and}$$
$$f\left(\tfrac{1}{2}\right) = 2\left\lfloor \tfrac{1}{2} + 1 \right\rfloor = 2\left\lfloor \tfrac{3}{2} \right\rfloor = 2 \times 1 = 2,$$

but $0 \neq \frac{1}{2}$.

(c) **No**, f is not onto since $\text{range}(f) \neq \mathbb{Z}$ (e.g. there is no $x \in \mathbb{Q}$ such that $f(x) = 1$ because 1 is odd).

(d) We have

$$(g \circ f)(x) = g(f(x)) = 2(2\lfloor x + 1 \rfloor) - 1 = 4\lfloor x + 1 \rfloor - 1.$$

(e) We have

$$(g \circ f)\left(-\frac{3}{4}\right) = 4 \cdot 0 - 1 = -1.$$

(f) The range is a subset of $\{4n - 1 \mid n \in \mathbb{Z}\}$ because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. This *is* the range because, given an integer $4n - 1$, we have $f(n - 1) = 4\lfloor n - 1 + 1 \rfloor - 1 = 4n - 1$. Note that you can also write the range as $\{n \in \mathbb{Z} \mid n \equiv -1 \pmod 4\}$ which is the same as $\{n \in \mathbb{Z} \mid n \equiv 3 \pmod 4\}$.

3. (a) The statement is **true**.

Proof. Suppose that f and $f \circ g$ are one-to-one functions. Suppose for a contradiction that g is not one-to-one. Thus there exist two distinct elements in the domain of g, say x_1 and x_2, for which $g(x_1) = g(x_2)$. Let $g(x_1) = y = g(x_2)$. Thus $f(g(x_1)) = f(y) = f(g(x_2))$, but $x_1 \neq x_2$, which contradicts the fact that $f \circ g$ is one-to-one. Therefore g must be one-to-one. □

(b) The statement is **false**.

Counterexample. Consider the functions $g : \{1\} \to \{2, 3\}$ defined by $g(1) = 2$, and $f : \{2, 3\} \to \{4\}$ defined by $f(2) = 4$ and $f(3) = 4$. Then f is onto, and $f \circ g$ is onto (since $f \circ g : \{1\} \to \{4\}$ and $f(g(1)) = 4$). However, g is not onto. □

§27 — Cardinalities

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 21 (week 8).

Problems

1. Let $A = \{-2, -1, 0, 1\}$ and $B = \{3, 4, 5, 6\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.
2. Prove that $|\{1, 2, 3\}| \leq |\mathbb{Z}|$ by providing an appropriate injective (one-to-one) function.
3. Consider the intervals

$$[6, 12] = \{x \in \mathbb{R} \mid 6 \leq x \leq 12\} \quad \text{and} \quad (6, 12) = \{x \in \mathbb{R} \mid 6 < x < 12\}.$$

   Prove that $|[6, 12]| \leq |(6, 12)|$ by providing an appropriate injective (one-to-one) function.
4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.

Solutions

1. Define the function $f : A \to B$ by

$$f(-2) = 3, \qquad f(-1) = 4, \qquad f(0) = 5, \qquad f(1) = 6.$$

   Then f is bijective, hence $|A| = |B|$.
2. Define the function $g : \{1, 2, 3\} \to \mathbb{Z}$ by $g(1) = 1$, $g(2) = 2$, and $g(3) = 3$. Then g is injective (one-to-one), so $|\{1, 2, 3\}| \leq |\mathbb{Z}|$.

3. Define $h : [6, 12] \to (6, 12)$ by

$$h(x) = \frac{x}{2} + 4.$$

For each $x \in [6, 12]$ we have

$$\begin{aligned} \frac{6}{2} + 4 \leq h(x) &\leq \frac{12}{2} + 4 \\ 7 \leq h(x) &\leq 10. \end{aligned}$$

Thus h is indeed a function from $[6, 12]$ to $(6, 12)$, and h has range $[7, 10] \subseteq (6, 12)$.

Suppose $x, y \in [6, 12]$ and $h(x) = h(y)$. Then $\frac{x}{2} + 4 = \frac{y}{2} + 4$, so $x = y$. Therefore h is injective (one-to-one).

Thus $|[6, 12]| \leq |(6, 12)|$.

4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$.

Consider the function $f : A \to B$ where $f(x) = 2x + 5$. Since $x \geq -1$, $f(x) = 2x + 5 \geq 2(-1) + 5 = 3$, and since $x \leq 1$, $f(x) = 2x + 5 \leq 2(1) + 5 = 7$. Also each value of x gives a unique value of $2x + 5$. Thus f is a function with the correct domain and codomain.

We now prove that f is one-to-one. Suppose that $x_1, x_2 \in A$ and $f(x_1) = f(x_2)$. Thus $2x_1 + 5 = 2x_2 + 5$, and so $x_1 = x_2$. Thus f is one-to-one.

We now prove that f is onto. Suppose $y \in [3, 7]$. Let $x = \frac{y-5}{2}$. Since $y \leq 7$, we have $x \leq 1$ and since $y \geq 3$, we have $x \geq -1$. So $x \in [-1, 1]$. Furthermore $f(x) = f\left(\frac{y-5}{2}\right) = 2\left(\frac{y-5}{2}\right) + 5 = y - 5 + 5 = y$. Thus f is onto.

Hence f is a bijection and so $|A| = |B|$.

§28 — Countable and Uncountable Sets

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 22 (week 8).

Note that this content will not be assessed in MATH1061.

Problems

1. Determine whether each of the following sets is countable or uncountable.
   (a) $\{1, 2, \ldots, n\}$.
   (b) $\mathbb{Z} \times \mathbb{Z}$.
   (c) $\mathbb{Q} \times \mathbb{Q}$.
   (d) $\mathbb{Z} \times \mathbb{Z} \times \cdots$ (infinitely many copies of $\mathbb{Z}$).
2. (a) Is $|\mathbb{Z}| = |\mathbb{Q}|$?
   (b) Is $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$?
   (c) Is $|\mathbb{R}| = |\mathbb{Q} \times \mathbb{Q}|$?
3. (a) Show that the union of a countable number of countable sets is countable.
   (b) Show that the set of all finite binary strings is countable.
   (c) Use (a) to show that the set of all irrational numbers is uncountable.

Solutions

1. (a) The set is **countable** because the function $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ defined by $f(i) = i$ is injective.
   (b) The set $\mathbb{Z} \times \mathbb{Z}$ is **countable**. Define the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ by

$$f(a,b) = \begin{cases} 2^a 3^b, & a > 0,\ b > 0, \\ 5^{-a} 7^{-b}, & a < 0,\ b < 0, \\ 11^a 13^{-b}, & a > 0,\ b < 0, \\ 17^{-a} 19^b, & a < 0,\ b > 0, \\ 23^b, & a = 0,\ b > 0, \\ 29^a, & a > 0,\ b = 0, \\ 31^{-b}, & a = 0,\ b < 0, \\ 37^{-a}, & a < 0,\ b = 0, \\ 1, & (a,b) = (0,0). \end{cases}$$

   We claim f is injective. Suppose $f(a,b) = f(c,d)$. By unique prime factorisation, the set of primes dividing $f(a,b)$ and the set of primes dividing $f(c,d)$ must be equal. Hence (a,b) and (c,d) lie in the same case. Again, by unique prime factorisation, the corresponding exponents must agree, so $a = c$ and $b = d$. Therefore f is injective.

(c) The set $\mathbb{Q} \times \mathbb{Q}$ is **countable**. First define an injection $e : \mathbb{Z} \to \mathbb{N}$ by

$$e(z) = \begin{cases} 2z, & z \geq 0, \\ -2z - 1, & z < 0. \end{cases}$$

Next define an injection $c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by

$$c(m, n) = 2^m 3^n.$$

Write each rational in lowest terms with positive denominator: $x = \frac{p}{q}$, $y = \frac{r}{s}$ with $p, r \in \mathbb{Z}$ and $q, s \in \mathbb{N}$. Define $F : \mathbb{Q} \times \mathbb{Q} \to \mathbb{N}$ by

$$F\left(\frac{p}{q}, \frac{r}{s}\right) = 2^{\,c(e(p),\, q)}\, 3^{\,c(e(r),\, s)}.$$

If $F\left(\frac{p}{q}, \frac{r}{s}\right) = F\left(\frac{p'}{q'}, \frac{r'}{s'}\right)$, then by unique prime factorisation we get $c(e(p), q) = c(e(p'), q')$ and $c(e(r), s) = c(e(r'), s')$. Since c is injective, we have $e(p) = e(p')$, $q = q'$, $e(r) = e(r')$, $s = s'$. Moreover, since e is injective, we have $p = p'$ and $r = r'$. Therefore $\frac{p}{q} = \frac{p'}{q'}$ and $\frac{r}{s} = \frac{r'}{s'}$, so F is injective.

(d) The set $\mathbb{Z} \times \mathbb{Z} \times ...$ is **not countable**. We will prove this by giving an injection $\mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$.

For each $x \in \mathbb{R}$, write $x = n + r$ with $n = \lfloor x \rfloor \in \mathbb{Z}$ and $r \in [0, 1)$. Choose the unique decimal expansion of r that does not end with an infinite tail of 9's. Write this decimal expansion as

$$r = 0.d_1 d_2 d_3 \cdots, \qquad d_k \in \{0, 1, \ldots, 9\}.$$

Then define the function $\iota : \mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$ by

$$\iota(x) = (n, d_1, d_2, d_3, \ldots) \in \mathbb{Z} \times \mathbb{Z} \times \cdots.$$

This is injective; if $\iota(x) = \iota(y)$ then the decimals of x and y are equal, so $x = y$.

2. (a) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Q}$ are countable and infinite.

   (b) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are countable and infinite.

   (c) **No.** $\mathbb{Q} \times \mathbb{Q}$ is countable, while $\mathbb{R}$ is uncountable.

3. (a) Let $A_1, A_2, A_3, ...$ be countable. Then for each n we can list A_n as

$$A_n = \{a_{n,1}, a_{n,2}, a_{n,3}, ...\}.$$

Now list the union by going along diagonals:

$$a_{1,1};\ a_{1,2}, a_{2,1};\ a_{1,3}, a_{2,2}, a_{3,1};\ a_{1,4}, a_{2,3}, a_{3,2}, a_{4,1};\ ...$$

Every element of every A_n appears somewhere in this list, so $\bigcup_{n=1}^{\infty} A_n$ can be listed in a sequence. Hence $\bigcup_{n=1}^{\infty} A_n$ is countable.

(b) Let B_n be the set of all binary strings of length n. Each B_n is finite (there are 2^n such strings), hence countable. Every finite binary string has some length, so

$$B = \{\text{all finite binary strings}\} = \bigcup_{n=0}^{\infty} B_n.$$

By (a), a countable union of countable sets is countable, so B is countable.

(c) Suppose, for contradiction, that the set of irrationals $\mathbb{R} \setminus \mathbb{Q}$ were countable. We already know $\mathbb{Q}$ is countable. Then by part (a),

$$\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$$

would be a union of two countable sets, hence countable. But $\mathbb{R}$ is uncountable. This contradiction shows that $\mathbb{R} \setminus \mathbb{Q}$ is uncountable.

Application — Computability of Functions

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 170–177.*

An important application of the topic of countability to computer science is examining the **computability** of functions. In computer science, a function is **computable** if there is a computer program in some programming language that can find the values of the function. If there is no such program, we say the function is **uncomputable**.

Application problems

1. (a) Show the set of all computer programs in any given computer language is countable.

   Hint: a computer program written in a programming language can be thought of as a string of symbols from a finite alphabet.

   (b) Let T be the set of all functions from $\mathbb{Z}^+$ to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Show that T is uncountable.

   Hint: start by finding an injection between the interval $(0, 1)$ *and a subset of* T*.*

   (c) Hence show that there are uncomputable functions.

Application solutions

1. (a) Given a computer language with a finite alphabet A, we let P be the set of all computer programs in the language. If P is finite, then it is countable and we are done, so assume P is infinite.

   Now we use the fact that we can think of each computer program as a series of strings made using the alphabet A. Consider all strings of length m made from alphabet A, and denote this set by A_m. It is easy to show that there are $|A|^m$ distinct strings of this type, and since A is finite, $|A|^m$ is also finite. Now P is a subset of $\bigcup_{i=1}^{\infty} A_m$. Since the union of a countable number of countable sets is also countable (see Question 3(a) from earlier in this section) it follows that $\bigcup_{i=1}^{\infty} A_m$ is countable and hence P is countable.

   (b) We use the hint and start by defining a function from $(0, 1)$ to T as follows. Recall that every real number in the interval $(0, 1)$ can be written in decimal notation as $0.a_1a_2a_3 \ldots a_n \ldots$ where each a_i is an integer from 0 to 9. Also recall that T is the set of all functions from $\mathbb{Z}^+$ to $\{0, 1, \ldots, 9\}$. Let $f : (0, 1) \to T$ be the function defined as

   $$f(0.a_1a_2a_3 \ldots a_n \ldots) = g,$$

   where g is the function in T such that $g(n) = a_n$ for all $n \in \mathbb{Z}^+$.

   So for example, if $f(0.457013) = g$ then g is the function where $g(1) = 4$, $g(2) = 5$, $g(3) = 7$, $g(4) = 0$, $g(5) = 1$, $g(6) = 3$ and $g(n) = 0$ for all $n \geq 7$.

   Now we will prove that this function is one-to-one. Suppose that $f(x_1) = f(x_2)$ for $x_1, x_2 \in (0, 1)$. Then for these functions to be equal, they map every integer to the same value. For this to happen, every decimal digit of x_1 must be equal to the same decimal digit of x_2 and so we must have $x_1 = x_2$.

   Now denote the set of all outputs of f as S. Hence $S \subseteq T$. Now if we set the codomain of f to be S, which is the range of f, we have made this function surjective and hence a

bijection. This means that the subset $S \subseteq T$ is in bijection with the interval $(0, 1)$. Since the interval $(0, 1)$ is uncountable, we must have that S is also uncountable and since $S \subseteq T$, T must also be uncountable.

(c) Part (a) showed us that the set of all computer programs in a given language is countable. This means that there are a countable number of computable functions. However part (b) showed us that there is an uncountable number of functions in the set T, so we must have that some functions are uncomputable.

§29 — Relations on Sets

Epp 4th ed. pp. 442–449 · 5th ed. (metric) pp. 487–494. Lecture 23 (week 8).

Problems

1. Define a relation P on $\mathbb{Z}$ as follows: for every ordered pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$,

$$m \; P \; n \iff m \text{ and } n \text{ have a common prime factor.}$$

   (a) Is $15 \; P \; 25$?

   (b) Is $22 \; P \; 27$?

   (c) Is $0 \; P \; 5$?

   (d) Is $8 \; P \; 8$?

2. Let $X = \{a, b, c\}$. Define a relation S on the power set $\mathcal{P}(X)$ as follows: for all sets A and B in $\mathcal{P}(X)$,

$$A \; S \; B \iff A \text{ has the same number of elements as } B.$$

   (a) Is $\{a, b\} \; S \; \{b, c\}$?

   (b) Is $\{a\} \; S \; \{a, b\}$?

   (c) Is $\{c\} \; S \; \{b\}$?

3. Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ be sets. Let R be the 'divides' relation. That is, for every ordered pair (a, b) in $A \times B$, we have $a \; R \; b$ if and only if $a \mid b$. Draw an arrow diagram (i.e. the directed graph) of this relation.

Solutions

1. (a) **Yes**, since $15 = 3 \cdot 5$ and $25 = 5 \cdot 5$ share the prime factor 5.

   (b) **No**, since $22 = 2 \cdot 11$ and $27 = 3^3$ share no common prime factor.

   (c) **Yes**, since 0 is divisible by every prime; in particular $5 \mid 0$ and $5 \mid 5$, so 0 and 5 have a common prime factor.

   (d) **Yes**, since $8 = 2^3$ and 2 is a prime factor of 8 (so they share the prime factor 2).

2. (a) **Yes**, since $|\{a, b\}| = 2 = |\{b, c\}|$.

   (b) **No**, since $|\{a\}| = 1 \neq 2 = |\{a, b\}|$.

   (c) **Yes**, since $|\{c\}| = 1 = |\{b\}|$.

3. We have $A \times B = \{(3,4), (3,5), (3,6), (4,4), (4,5), (4,6), (5,4), (5,5), (5,6)\}$. The pairs (a, b) satisfying $a \mid b$ are

$$\{(3,6),\ (4,4),\ (5,5)\} \subseteq A \times B.$$

   So the directed graph has an arrow from 3 (in A) to 6 (in B), an arrow from 4 to 4, and an arrow from 5 to 5 — and no other arrows.

§30 — Reflexivity, Symmetry, Transitivity

Epp 4th ed. pp. 449–459 · 5th ed. (metric) pp. 495–505. Lecture 23 (week 8).

Problems

1. Let $X = \{1, 2, 3, 4, 5\}$ and consider the subset $R \subseteq X \times X$ given by

$$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,3), (3,4), (4,5), (5,1)\}.$$

   (a) Draw an arrow diagram for the binary relation R.

   (b) Draw an arrow diagram for the binary relation R^{-1}.

   (c) Draw an arrow diagram for the binary relation $R \cup R^{-1}$.

   (d) Is R symmetric? Is R^{-1} symmetric? Is $R \cup R^{-1}$ symmetric?

   (e) Is R transitive? Is R^{-1} transitive? Is $R \cup R^{-1}$ transitive?

2. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:

- $(1, 2) \in R$
- $(2, 3) \in R$
- R is reflexive
- R is transitive

What is the minimum number of arrows required in an arrow diagram for a relation R that satisfies these criteria?

Solutions

1. (a) The arrow diagram for R has the five vertices $1, 2, 3, 4, 5$ drawn around a circle, with a **loop at every vertex** (from the pairs $(1, 1), \ldots, (5, 5)$) together with the directed 5-cycle

$$1 \to 2 \to 3 \to 4 \to 5 \to 1.$$

(b) The arrow diagram for R^{-1} is the same picture with every non-loop arrow reversed: a loop at every vertex, together with the directed 5-cycle

$$1 \to 5 \to 4 \to 3 \to 2 \to 1,$$

that is, $R^{-1} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (2, 1), (3, 2), (4, 3), (5, 4), (1, 5)\}$.

(c) The arrow diagram for $R \cup R^{-1}$ has a loop at every vertex and a **double-headed arrow** between each consecutive pair around the cycle — that is, both $(i, i + 1)$ and $(i + 1, i)$ for the cycle $1, 2, 3, 4, 5, 1$.

(d) R is **not** symmetric because $(1, 2) \in R$ but $(2, 1) \notin R$.

R^{-1} is **not** symmetric because $(2, 1) \in R^{-1}$ but $(1, 2) \notin R^{-1}$.

$R \cup R^{-1}$ **is** symmetric. If $(a, b) \in R \cup R^{-1}$ then $(a, b) \in R$ or $(a, b) \in R^{-1}$, which means $(b, a) \in R^{-1}$ or $(b, a) \in R$, and thus, in either case, $(b, a) \in R \cup R^{-1}$.

(e) R is **not** transitive because $(1, 2), (2, 3) \in R$ but $(1, 3) \notin R$.

R^{-1} is **not** transitive because $(3, 2), (2, 1) \in R^{-1}$ but $(3, 1) \notin R^{-1}$.

$R \cup R^{-1}$ is **not** transitive because $(1, 2), (2, 3) \in R \cup R^{-1}$ but $(1, 3) \notin R \cup R^{-1}$.

2. R is reflexive, so $(1,1),(2,2),(3,3) \in R$ — a loop on each point of the arrow diagram. We are also given $(1,2),(2,3) \in R$, and R is transitive, so $(1,3) \in R$. R is *not* required to be symmetric, so no further arrows are forced.

$$R = \{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3)\}$$

So the **minimum number of arrows required is 6**.

§31 — Equivalence Relations

Epp 4th ed. pp. 459–478 · 5th ed. (metric) pp. 505–523. Lecture 24 (week 9).

Problems

1. Define the binary relations α, β and γ on $\mathbb{Z}$ as follows:

$$\begin{aligned} x \,\alpha\, y &\iff x + y \text{ is an even integer,} \\ x \,\beta\, y &\iff x \text{ is a multiple of } y, \\ x \,\gamma\, y &\iff 3 \text{ is a factor of } x^2 - y^2. \end{aligned}$$

   (a) Fill in the table with 'Yes'/'No' to indicate the properties satisfied by each relation.

	α	β	γ
Reflexive			
Symmetric			
Transitive			
Equivalence relation			

   (b) For each equivalence relation, state its equivalence classes.

2. Let $A = \{a,b,c,d,e\}$ be a set and ρ be a binary relation defined by

$$\rho = \{(a,a),(a,b),(a,d),(b,b),(c,c),(d,d),(b,a),(d,a),(b,d),(d,b),(c,e),(e,c),(e,e)\}.$$

   For instance, $(a,b) \in \rho$ means $a \,\rho\, b$.

   (a) Draw the directed graph representing ρ.

   (b) Is ρ reflexive? Is ρ symmetric? Is ρ transitive?

(c) Is ρ an equivalence relation on A? If so, give its equivalence classes.

(d) What is the smallest subset τ of ρ which forms an equivalence relation on A?

(e) Give the equivalence classes for τ.

3. Consider a positive integer n and any set of strings S. Define a relation R_n on S by the condition $s\ R_n\ t$ if and only if $s = t$ or both s and t have at least n characters and the first n characters are the same. Show that R_n is an equivalence relation.

Solutions

1. (a)

	α	β	γ
Reflexive	Yes	Yes	Yes
Symmetric	Yes	No	Yes
Transitive	Yes	Yes	Yes
Equivalence relation	Yes	No	Yes

(b) The equivalence relations are α and γ.

For α, notice $x\ \alpha\ y \iff x + y$ is even $\iff x$ and y have the same parity. This means the equivalence classes are $\mathbb{Z}^{\text{even}}$ and $\mathbb{Z}^{\text{odd}}$.

For γ, notice $x\ \gamma\ y \iff 3 \mid (x^2 - y^2) \iff x^2 \equiv y^2 \pmod 3$. But modulo 3 the only possible square residues are

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 1 \pmod 3.$$

Hence $x^2 \equiv 0 \pmod 3$ exactly when $3 \mid x$, and $x^2 \equiv 1 \pmod 3$ exactly when $3 \nmid x$. Therefore $x\ \gamma\ y$ iff either both x and y are multiples of 3, or neither is. So the equivalence classes are $\{n \in \mathbb{Z} : 3 \mid n\}$ and $\{n \in \mathbb{Z} : 3 \nmid n\}$. Note that another way to write the equivalence classes is $\{3n \mid n \in \mathbb{Z}\}$ and $\{3n + 1,\ 3n + 2 \mid n \in \mathbb{Z}\}$.

2. (a) A digraph for ρ (vertex set $A = \{a, b, c, d, e\}$) has a **loop at every vertex**, double-headed arrows between each pair of $\{a, b, d\}$ — that is between a and b, between a and d, and between b and d — and a double-headed arrow between c and e. There are no arrows between $\{a, b, d\}$ and $\{c, e\}$.

(b) ρ is **reflexive**: we have $(x, x) \in \rho$ for all $x \in A$ (loops on all vertices).

ρ is **symmetric**: whenever $(x, y) \in \rho$, we have $(y, x) \in \rho$ (no single-direction arrow between any two distinct vertices).

ρ is **transitive**: within $\{a, b, d\}$ all relations occur, within $\{c, e\}$ all relations occur, and there are no relations between $\{a, b, d\}$ and $\{c, e\}$. That is, whenever (x, y) and (y, z) are in ρ, then (x, z) is also in ρ (and $x = z$ is possible).

(c) **Yes**, ρ is an equivalence relation. Its equivalence classes are

$$[a] = [b] = [d] = \{a, b, d\}, \qquad [c] = [e] = \{c, e\}.$$

(d) An equivalence relation $\tau \subseteq \rho$ must be reflexive, so $(x, x) \in \tau$ for all $x \in A$. But notice if τ is the relation

$$\tau = \{(a, a), (b, b), (c, c), (d, d), (e, e)\}$$

then τ is an equivalence relation. Therefore this is the smallest relation which is an equivalence relation.

(e) The equivalence classes for τ are the singletons:

$$[a] = \{a\},\ [b] = \{b\},\ [c] = \{c\},\ [d] = \{d\},\ [e] = \{e\}.$$

3. Let S be any set of strings and fix $n \in \mathbb{Z}^+$.

   R_n **is reflexive:** for any $s \in S$, since $s = s$, by definition $s\ R_n\ s$.

   R_n **is symmetric:** let $s, t \in S$, and assume $s\ R_n\ t$. If $s = t$ then $t\ R_n\ s$; otherwise both s and t must have at least n characters and, since $s\ R_n\ t$, they must have the same first n characters, so $t\ R_n\ s$.

   R_n **is transitive:** let $s, t, u \in S$ and assume $s\ R_n\ t$ and $t\ R_n\ u$. Since $s\ R_n\ t$ we either have $s = t$, or s and t both have at least n characters and have the same first n characters. Similarly, since $t\ R_n\ u$, either $t = u$, or t and u both have at least n characters and have the same first n characters. Thus either $s = t = u$, or s and u both have at least n characters and they both share the first n characters with t (and hence each other). Thus $s\ R_n\ u$ and so R_n is transitive.

   Since R_n is reflexive, symmetric and transitive it is an equivalence relation. □

Application — Identifiers

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 608–618.*

In the C programming language, an **identifier** is the name of a variable, a function or another type of entity.

Each identifier is a nonempty string of characters where each character is a lowercase or uppercase English letter, a digit, or an underscore.

There is no limit on the number of characters used in the identifier; however, for some compilers for some versions of C, there is a limit on the number of characters checked when two names are compared.

For example, Standard C compilers consider two identifiers the same when they agree in their first 31 characters. We see that two identifiers will be considered the same if and only if they are related under the relation R_n when $n = 31$ (defined in a previous question).

Application problems

1. Using R_{31} on the set of all possible identifiers, determine the equivalence classes of each of the following identifiers:

   (a) `file_1`

   (b) `Number_of_tropical_storms`

   (c) `Number_of_named_tropical_storms`

   (d) `Number_of_named_tropical_storms_in_the_Atlantic_in_2005`

Application solutions

1. Let I be the set of all possible identifiers (strings over letters, digits and underscores).

   (a) Since `file_1` has length $6 < 31$, its equivalence class is just

   $$[\texttt{file_1}]_{R_{31}} = \{\texttt{file_1}\}.$$

   (b) Since `Number_of_tropical_storms` has length $25 < 31$, its equivalence class is

   $$[\texttt{Number_of_tropical_storms}]_{R_{31}} = \{\texttt{Number_of_tropical_storms}\}.$$

(c) The identifier `Number_of_named_tropical_storms` has length exactly 31, so two identifiers are R_{31}-equivalent to it iff they have at least 31 characters and their first 31 characters equal this string. Hence

$$[\texttt{Number_of_named_tropical_storms}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 31 characters of} \\ t \text{ are } \texttt{Number_of_named_tropical_storms} \end{array} \right\}.$$

(d) The identifier `Number_of_named_tropical_storms_in_the_Atlantic_in_2005` begins with the same first 31 characters `Number_of_named_tropical_storms`, so it has the same R_{31}-equivalence class as in (c):

$$[\texttt{Number_of_named_tropical_storms_in_the_Atlantic_in_2005}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 3} \\ t \text{ are } \texttt{Number_of_name} \end{array} \right.$$

§32 — Partial Order Relations

Epp 4th ed. pp. 498–515 · 5th ed. (metric) pp. 546–563. Lecture 25 (week 9).

Problems

1. Let ρ be a relation on $\mathbb{Z}$ defined by $x \rho y$ if and only if $x^3 - 1 < y^3$.
   (a) Prove ρ is a partial order relation.
   (b) Is ρ a total order?
2. Let S be the set of binary strings of length 6. Define the **weight** of a binary string as the number of ones it contains. (For example, weight(110110) = 4.) Define a relation ρ on S by

   $$s \rho t \text{ if and only if } \text{weight}(s) \leq \text{weight}(t).$$

   (a) Prove that ρ is not an equivalence relation.
   (b) Prove that ρ is not a partial order relation.
3. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:
   - $(2, 3) \in R$
   - $(3, 2) \in R$
   - $(1, 1) \notin R$

- R is transitive
- R is not symmetric
- R is not antisymmetric.

Draw an arrow diagram for the relation R.

Solutions

1. (a) To show that ρ is a partial order, we need to show that ρ is reflexive, antisymmetric and transitive.

   Reflexive: let $x \in \mathbb{Z}$. Then $x^3 - 1 < x^3$ and so $x \rho x$, so ρ is reflexive.

   Antisymmetric: suppose $x \rho y$ where $x \neq y$. (We must show that then $y \not\rho x$.) Now $x \rho y$ means that $x^3 - 1 < y^3$. And since $x \neq y$ we must have $x^3 < y^3$ and so $x^3 \leqslant y^3 - 1$. Hence $y^3 - 1 \not< x^3$ and so we do not have $y \rho x$. Therefore ρ is antisymmetric.

   Transitive: suppose that $x \rho y$ and $y \rho z$. Then we know that $x^3 - 1 < y^3$ and $y^3 - 1 < z^3$. So $x^3 - 1 \leqslant y^3 - 1 < z^3$, that is, $x^3 - 1 < z^3$ so that $x \rho z$, which means that ρ is transitive.

   Hence ρ is a partial order. □

   (b) To check whether ρ is a total order, let x and y be any two distinct integers. Then $x^3 \neq y^3$ and so either $x^3 < y^3$ or else $y^3 < x^3$.

   If $x^3 < y^3$ then $x^3 - 1 < y^3$ and so $x \rho y$.

   If $y^3 < x^3$ then $y^3 - 1 < x^3$ and so $y \rho x$.

   So for any integers $x \neq y$, we have either $x \rho y$ or else $y \rho x$. So any two integers are comparable under ρ. Hence ρ **is** a total order.

2. (a) It is **not an equivalence relation** because it is not symmetric. For instance, let $s = 000000$ and $t = 111111$. Then $\text{weight}(s) = 0 \leq 6 = \text{weight}(t)$, so $(s, t) \in \rho$, but $(t, s) \notin \rho$.

   (b) It is **not a partial order** because it is not antisymmetric. For instance, let $s = 100000$ and $t = 010000$. Then $\text{weight}(s) = \text{weight}(t) = 1$, so $s \rho t$ and $t \rho s$, but $s \neq t$.

3. One relation on $\{1, 2, 3\}$ satisfying all conditions is

$$R = \{(1, 2), (1, 3), (2, 2), (3, 3), (2, 3), (3, 2)\}.$$

(It contains $(2,3)$ and $(3,2)$; it is transitive; it is not symmetric since $(1,2) \in R$ but $(2,1) \notin R$; it is not antisymmetric since $2 \neq 3$ and $(2,3),(3,2) \in R$; and $(1,1) \notin R$.)

An arrow diagram for this R has vertices $1,2,3$ with: arrows $1 \to 2$ and $1 \to 3$; loops at 2 and at 3; and a double-headed arrow between 2 and 3. There is no loop at vertex 1.

§33 — Definitions and Examples of Groups

No relevant textbook pages. Lecture 26 (week 9).

Problems

1. Show $\mathbb{Z}_9 - \{0\} = \{1,2,3,\ldots,7,8\}$ is not a group under multiplication modulo 9.
2. Let G be the set of all odd integers. Define the binary operation $\star$ on G by

$$x \star y = x + y - 1.$$

   Show that $(G, \star)$ is an abelian group.
3. Show $\mathbb{Z}_9 - \{0,3,6\} = \{1,2,4,5,7,8\}$ is a group under multiplication modulo 9. Is the group abelian?
4. Define the group $H = \mathbb{Z}_5 - \{0\} = \{1,2,3,4\}$ under multiplication modulo 5. Write the Cayley table for H.
5. Define the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ under component-wise addition modulo 2. That is,

$$(a,b) + (c,d) = (a + c \bmod 2,\ b + d \bmod 2).$$

   Write the Cayley table for G.

Solutions

1. It is not a group under multiplication mod 9 because, for example, it is **not closed** ($3 \cdot 3 = 0 \notin \mathbb{Z}_9 - \{0\}$).

2. **Closure:** if x and y are odd, then $x+y$ is even, so $x+y-1$ is odd. Hence $x \star y \in G$.

   Associativity: for $x, y, z \in G$,

$$(x \star y) \star z = (x+y-1)+z-1 = x+y+z-2 = x+(y+z-1)-1 = x \star (y \star z).$$

   Commutativity: for $x, y \in G$,

$$x \star y = x+y-1 = y+x-1 = y \star x.$$

   Identity: we seek $e \in G$ such that $x \star e = x = e \star x$ for all x. Now the requirement $x \star e = x+e-1 = x$ implies that $e = 1$. Note 1 lies in G. Moreover, commutativity implies that $e \star x = x$ as well. Thus the identity is 1.

   Inverses: given $x \in G$, we want $y \in G$ with $x \star y = 1$. This means $x+y-1 = 1$, so $y = 2-x$. Since x is odd, $2-x$ is odd, hence $2-x \in G$. Thus the inverse of x is $x^{-1} = 2-x$.

   Therefore $(G, \star)$ is an abelian group. $\square$

3. **Closure:** if $a, b \in \{1,2,4,5,7,8\}$, then $3 \nmid a$ and $3 \nmid b$, hence $3 \nmid ab$, so $ab \not\equiv 0, 3, 6 \pmod 9$; thus $\{1,2,4,5,7,8\}$ is closed under multiplication modulo 9.

   Associativity and commutativity: normal multiplication between integers is associative and commutative, so multiplication modulo 9 in the set $\{1,2,4,5,7,8\}$ is also associative and commutative. This means the group **is abelian**.

   Identity: $1 \in G$ is the identity because $1 \cdot x \equiv x \pmod 9$.

   Inverse: every element has an inverse. We explicitly calculate the inverses:

$$\begin{aligned}
1^{-1} &= 1 \quad \text{because } 1 \cdot 1 \equiv 1 \pmod 9,\\
2^{-1} &= 5 \quad \text{because } 2 \cdot 5 = 10 \equiv 1 \pmod 9,\\
4^{-1} &= 7 \quad \text{because } 4 \cdot 7 = 28 \equiv 1 \pmod 9,\\
5^{-1} &= 2 \quad \text{because } 5 \cdot 2 = 10 \equiv 1 \pmod 9,\\
7^{-1} &= 4 \quad \text{because } 7 \cdot 4 = 28 \equiv 1 \pmod 9,\\
8^{-1} &= 8 \quad \text{because } 8 \cdot 8 = 64 \equiv 1 \pmod 9.
\end{aligned}$$

4. For $H = \mathbb{Z}_5 \setminus \{0\} = \{1,2,3,4\}$ under multiplication mod 5, the Cayley table is:

$\cdot$	1	2	3	4
1	1	2	3	4

$\cdot$	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

5. For $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ under componentwise addition mod 2, the Cayley table is:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(\mathbf{1},\mathbf{0})$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(\mathbf{1},\mathbf{1})$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

§34 — Elementary Properties of Groups

No relevant textbook pages. Lecture 27 (week 10).

Problems

1. Let $H = \{3n \mid n \in \mathbb{Z}\}$ be the set of multiples of 3. Prove H is a subgroup of $(\mathbb{Z}, +)$.
2. Fix elements g and h in a group G where e is the group identity. Prove the following statements:
   (a) If $g^{-1} = h$ then $h^{-1} = g$.
   (b) $(g^{-1})^{-1} = g$.
   (c) $(gh)^{-1} = h^{-1}g^{-1}$.
3. Prove $K = \{(0,0),(0,1),(2,0),(2,1)\}$ is a subgroup of $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$ where the group operation is componentwise addition:

$$(a,b) + (c,d) = (a + c \pmod 4,\ b + d \pmod 2).$$

4. Consider the group $(\mathbb{Z}_{11} - \{0\}, \cdot)$. Show that this group is cyclic.
   Hint: express every element of $\mathbb{Z}_{11} - \{0\}$ as a power of 2.

Solutions

1. First we note that $H \subseteq \mathbb{Z}$, and $H \neq \emptyset$.

   Closure: if $x, y \in H$ then $x = 3a$ and $y = 3b$ for some $a, b \in \mathbb{Z}$. Therefore $x + y = 3a + 3b = 3(a + b) \in H$.

   Identity: the identity of $(\mathbb{Z}, +)$ is 0, and since $0 = 3 \cdot 0$, we have $0 \in H$.

   Inverse: in $\mathbb{Z}$, the inverse of x is $-x$. In H, if $x \in H$ then $x = 3a$ for some $a \in \mathbb{Z}$. This means $-x = -3a = 3 \cdot (-a)$, and so $-x \in H$ also.

   Note that we do not need to check associativity for subgroups, since this property is automatically inherited from the parent group $(\mathbb{Z}, +)$. □

2. (a) Suppose $g^{-1} = h$. Now $gh = gg^{-1} = e$ and $hg = g^{-1}g = e$. Thus $h^{-1} = g$.

   (b) By definition, $gg^{-1} = e = g^{-1}g$, so $(g^{-1})^{-1} = g$.

   (c) Notice we have

   $$(gh)(h^{-1}g^{-1}) = ghh^{-1}g^{-1} = e$$

   and

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

   This means $(gh)^{-1} = h^{-1}g^{-1}$.

3. We draw the Cayley table of $K = \{(0,0), (0,1), (2,0), (2,1)\}$ under componentwise addition in $\mathbb{Z}_4 \times \mathbb{Z}_2$:

$+$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(2,1)$	$(2,0)$
$(\mathbf{2},\mathbf{0})$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$
$(\mathbf{2},\mathbf{1})$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$

   Notice the operation is closed in K and every element of K has an inverse in K. Therefore K is a subgroup. □

4. Note that 2 is a generator of $(\mathbb{Z}_{11} - \{0\}, \cdot)$, so it is cyclic:

   $$1 = 2^0,\ 2 = 2^1,\ 4 = 2^2,\ 8 = 2^3,\ 5 = 2^4,\ 10 = 2^5,\ 9 = 2^6,\ 7 = 2^7,\ 3 = 2^8,\ 6 = 2^9.$$

§35 — Group Isomorphisms

No relevant textbook pages. No lecture in the published schedule — the Week 10 row jumps from L27 (V34) to L28 (V36).

This content is optional and will not be assessed. The source document carries no practice problems or solutions for this section.

§36 — Definitions and Examples of Fields

No relevant textbook pages. Lecture 28 (week 10).

Problems

1. (a) Solve $3x + 4 = 2$ in the field $(\mathbb{Z}_5, +, \cdot)$.
   (b) Solve $8x - 9 = 6$ in the field $(\mathbb{Z}_{11}, +, \cdot)$.
   (c) Solve $4(1 - x) = 10$ in the field $(\mathbb{Z}_{13}, +, \cdot)$.
   (d) Solve $16(x - 6) = 15$ in the field $(\mathbb{Z}_{19}, +, \cdot)$.
2. Prove $\mathbb{Z}_{12}$ with addition modulo 12 and multiplication modulo 12 is not a field.
3. Define addition and multiplication on $\mathbb{Q} \times \mathbb{Q}$ by

$$(a, b) + (c, d) = (a + c,\ b + d)$$

   and

$$(a, b) \cdot (c, d) = (ac + 3bd,\ ad + bc)$$

   for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$. Prove that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field.

Solutions

1. (a)

$$\begin{aligned} 3x + 4 &= 2 \\ \rightarrow 3x &= -2 \end{aligned}$$

Now, since $3 \times 2 = 6 \equiv 1 \pmod 5$, 2 is the multiplicative inverse of 3, and so we multiply both sides by 2 and obtain $x = -4$. That is, $x = 1$.

Check: $3 \cdot 1 + 4 = 7 \equiv 2 \pmod 5$.

(b)

$$\begin{aligned} 8x - 9 &= 6 \\ \rightarrow 8x &= 15 = 4 \end{aligned}$$

Now, since $8 \times 7 = 56 \equiv 1 \pmod{11}$, 7 is the multiplicative inverse of 8, and so we multiply both sides by 7 and obtain $x = 28$. That is, $x = 6$.

Check: $8 \cdot 6 - 9 = 39 \equiv 6 \pmod{11}$.

(c) Since $4 \times 10 = 40 \equiv 1 \pmod{13}$, 10 is the multiplicative inverse of 4, and so we multiply both sides by 10 and obtain $1 - x = 100 = 9$. That is, $x = 1 - 9 = 14 - 9 = 5$.

Check: $4(1 - 5) = -16 \equiv 10 \pmod{13}$.

(d) Since $16 \times 6 = 96 \equiv 1 \pmod{19}$, 6 is the multiplicative inverse of 16, and so we multiply both sides by 6 and obtain $x - 6 = 90 = 14$. That is, $x = 20 = 1$.

Check: $16(1 - 6) = -80 \equiv 15 \pmod{19}$.

2. $\mathbb{Z}_{12}$ is not a field because 2 has no multiplicative inverse modulo 12. Indeed $2 \cdot k \equiv 1 \pmod{12}$ has no solution since $2k$ is always even.

3. We show that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field in three steps.

Step 1 — $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Closure: for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a, b) + (c, d) = (a + c, b + d) \in \mathbb{Q} \times \mathbb{Q}$.

Associative: for all $(a, b), (c, d), (e, f) \in \mathbb{Q} \times \mathbb{Q}$ we have $\big((a, b) + (c, d)\big) + (e, f) = (a + c, b + d) + (e, f) = (a + c + e, b + d + f) = (a, b) + (c + e, d + f) = (a, b) + \big((c, d) + (e, f)\big)$.

Identity: for all $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b) = (0 + a, 0 + b) = (0, 0) + (a, b)$.

Inverses: for all $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a,b) + (-a,-b) = (a-a, b-b) = (0,0)$ and $(-a,-b) + (a,b) = (-a+a, -b+b) = (0,0)$. So $(-a,-b)$ is the inverse of (a,b).

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a,b) + (c,d) = (a+c, b+d) = (c+a, d+b) = (c,d) + (a,b)$.

Thus $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Step 2 — $((\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\},\ \cdot)$ is an abelian group.

Closure: for all $(a,b),(c,d) \in (\mathbb{Q}\times\mathbb{Q}) - \{(0,0)\}$, we have $(a,b)\cdot(c,d) = (ac+3bd, ad+bc) \in \mathbb{Q} \times \mathbb{Q}$. So we only need to show that $(ac+3bd, ad+bc) \neq (0,0)$. For a contradiction, suppose $(ac+3bd, ad+bc) = (0,0)$. That is, $ac+3bd = 0$ and $ad+bc = 0$. Multiplying the first equation by d and the second by c we obtain $acd + 3bd^2 = 0$ and $acd + bc^2 = 0$, from which it follows that $3bd^2 = bc^2$.

Now, if $b = 0$, then $ac = 0$, $ad = 0$ and $a \neq 0$, and so $c = d = 0$; a contradiction. Thus $b \neq 0$ and we have $3d^2 = c^2$. This is a contradiction because if $d = 0$, then $c \neq 0$ and the equation does not hold, and if $d \neq 0$, then we have $3 = \frac{c^2}{d^2}$, which implies $\sqrt{3} = \frac{c}{d}$ is rational. Thus $(ac+3bd, ad+bc) \neq (0,0)$ and we have closure.

Associative: for all $(a,b),(c,d),(e,f) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have

$$\begin{aligned}(a,b)\cdot\big((c,d)\cdot(e,f)\big) &= (a,b)\cdot(ce+3df,\ cf+de)\\ &= (a(ce+3df)+3b(cf+de),\ a(cf+de)+b(ce+3df))\\ &= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf)\end{aligned}$$

and

$$\begin{aligned}\big((a,b)\cdot(c,d)\big)\cdot(e,f) &= (ac+3bd,\ ad+bc)\cdot(e,f)\\ &= \big((ac+3bd)e+3(ad+bc)f,\ (ac+3bd)f+(ad+bc)e\big)\\ &= (ace+3bde+3adf+3bcf,\ acf+3bdf+ade+bce)\\ &= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf).\end{aligned}$$

Identity: for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have $(a,b)\cdot(1,0) = (a,b)$ and $(1,0)\cdot(a,b) = (a,b)$, so $(1,0)$ is a multiplicative identity.

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have

$$(a,b)\cdot(c,d) = (ac+3bd,\ ad+bc) = (ca+3db,\ cb+da) = (c,d)\cdot(a,b).$$

Inverses: we check that for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$,

$$(a,b)^{-1} = \left(\frac{a}{a^2-3b^2},\ \frac{-b}{a^2-3b^2}\right).$$

First, note that $a^2-3b^2 \neq 0$, because $a^2-3b^2=0$ implies either $(a,b)=(0,0)$ or $\sqrt{3}=\frac{a}{b}$, both of which are contradictions (the second because $\sqrt{3}$ is not rational). Thus $(a,b)^{-1} \in (\mathbb{Q}\times\mathbb{Q})-\{(0,0)\}$, and notice

$$\begin{aligned}(a,b)\cdot\left(\frac{a}{a^2-3b^2},\frac{-b}{a^2-3b^2}\right) &= \left(a\cdot\frac{a}{a^2-3b^2}+3b\cdot\frac{-b}{a^2-3b^2},\ a\cdot\frac{-b}{a^2-3b^2}+b\cdot\frac{a}{a^2-3b^2}\right)\\ &= \left(\frac{a^2-3b^2}{a^2-3b^2},\ \frac{-ab+ab}{a^2-3b^2}\right)\\ &= (1,0).\end{aligned}$$

So every nonzero element has an inverse. Thus $((\mathbb{Q}\times\mathbb{Q})-\{(0,0)\},\cdot)$ is an abelian group.

Step 3 — the distributive laws. For all $(a,b),(c,d),(e,f)\in\mathbb{Q}\times\mathbb{Q}$ we have

$$\begin{aligned}(a,b)\cdot((c,d)+(e,f)) &= (a,b)\cdot(c+e,\ d+f)\\ &= (a(c+e)+3b(d+f),\ a(d+f)+b(c+e))\\ &= ((ac+3bd)+(ae+3bf),\ (ad+bc)+(af+be))\\ &= (ac+3bd,\ ad+bc)+(ae+3bf,\ af+be)\\ &= (a,b)\cdot(c,d)+(a,b)\cdot(e,f)\end{aligned}$$

and (since we have already shown that multiplication and addition are commutative)

$$\begin{aligned}((a,b)+(c,d))\cdot(e,f) &= (e,f)\cdot((a,b)+(c,d))\\ &= (e,f)\cdot(a,b)+(e,f)\cdot(c,d) \quad \text{(by the first distributive law)}\\ &= (a,b)\cdot(e,f)+(c,d)\cdot(e,f).\end{aligned}$$

Thus $(\mathbb{Q}\times\mathbb{Q},+,\cdot)$ is a field. □

§37 — Introduction to Counting

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 29 (week 11).

Problems

1. The UQ drama club is auditioning for its annual production of *Romeo and Juliet*. Six people are auditioning for the role of Romeo, and eight other people are auditioning for the role of Juliet. In how many ways can the director cast the lead couple?
2. There are eleven questions on the final exam, but you decide — based on your successful grade for your in-semester exam — that you will only do five of them. How many combinations of questions are there which you could complete?
3. (a) How many permutations of $\{1, 2, \dots, 15\}$ start with an odd number?

   (b) How many 5-element subsets of $\{1, 2, \dots, 15\}$ contain exactly two numbers from $\{1, 2, 3, 4\}$?

Solutions

1. There are 6 choices for Romeo and 8 choices for Juliet, so $6 \cdot 8 = 48$ ways.
2. Since the order in which you do the 5 questions does not matter, there are $\binom{11}{5} = 462$ combinations of questions.
3. (a) There are 8 odd numbers in the set $\{1, \dots, 15\}$. Choose the first entry in 8 ways, then permute the remaining 14 numbers, so $8 \cdot 14!$ permutations.

   (b) We choose exactly 2 numbers from the set $\{1, 2, 3, 4\}$ and exactly 3 numbers from the remaining 11 numbers, so the number of subsets is

$$\binom{4}{2}\binom{11}{3}.$$

Application — Runtime

Not assessable for MATH1061. Taken from S. Epp, Discrete Mathematics with Applications, *5th edition, pages 787–799.*

In many algorithms, the runtime is well approximated by counting how many times the basic instructions are executed.

For programs with nested `for`-loops and no early exits, the total number of executions of the inner loop body equals the number of choices of the outer-loop index multiplied by the number of choices of the inner-loop index.

Concretely, if i runs through M values and, for each fixed i, the variable j runs through N values, then the inner loop body is executed exactly MN times.

Application problems

1. The following algorithms are written in pseudo-code and contain nested loops. For each algorithm, count the total number of iterations of the inner loop that the algorithm will run.

   (a)

```
for i := 1 to 30
    for j := 1 to 15
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (b)

```
for i := 5 to 50
    for j := 10 to 20
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (c) (Fix integers $a, b, c, d \in \mathbb{Z}^+$ with $a \leq b$ and $c \leq d$.)

```
for i := a to b
    for j := c to d
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

Application solutions

1. (a) $i = 1, \ldots, 30$ gives 30 iterations and $j = 1, \ldots, 15$ gives 15 iterations, so the inner loop runs $30 \cdot 15 = 450$ times.

   (b) $i = 5, \ldots, 50$ gives $50 - 5 + 1 = 46$ iterations and $j = 10, \ldots, 20$ gives $20 - 10 + 1 = 11$ iterations, so the inner loop runs $46 \cdot 11 = 506$ times.

   (c) $i = a, \ldots, b$ gives $b - a + 1$ iterations and $j = c, \ldots, d$ gives $d - c + 1$ iterations, so the inner loop runs $(b - a + 1)(d - c + 1)$ times.

§38 — Counting Selections

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 30 (week 11).

Problems

1. (a) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY?

   (b) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with R and end with P?

   (c) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with I and end with Y?

   (d) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that have all four Os next to each other?

2. (a) How many distinct arrangements can be made of the letters of the word WOOLLOONGABBA?

   (b) How many distinct arrangements are there of the letters of the word WOOLLOONGABBA such that **exactly one** of the following is true?

   - The two As are not next to each other.
   - The two Bs are not next to each other.
   - The two Ls are not next to each other.

3. (a) How many one-to-one (injective) functions are there from $\{a, b, c\}$ to $\{1, 2, 3, 4, 5\}$?

   (b) How many onto (surjective) functions are there from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$?

Solutions

1. (a) There are 13 letters in INDOOROOPILLY, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!} = 64\,864\,800.$$

   (b) Fix R in the first position and P in the last position. There are 11 letters remaining, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!\,2!} = 415\,800.$$

(c) Fix I in the first position and Y in the last position. There are 11 letters remaining, with four O's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!} = 831\,600.$$

(d) Treat the four O's as one 'letter'. There are 10 'letters' with two I's, two L's, and the remaining 'letters' appearing once each. Therefore the number of distinct arrangements is

$$\frac{10!}{2!\,2!} = 907\,200.$$

2. (a) There are 13 letters in WOOLLOONGABBA, with four O's, two L's, two A's, two B's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!\,2!} = 32\,432\,400.$$

(b) We want exactly one of the pairs AA, BB, LL to be non-adjacent. That is, there are three cases to consider:

- **Case 1:** the two A's are not adjacent but BB and LL are adjacent.
- **Case 2:** the two B's are not adjacent but AA and LL are adjacent.
- **Case 3:** the two L's are not adjacent but AA and BB are adjacent.

Note that the number of ways Case 1 can occur is exactly the same as the number of ways Case 2 can occur (and similarly for Case 3).

To count the number of ways Case 1 can occur, we first count arrangements with BB adjacent and LL adjacent. Treat BB as one 'letter' and LL as one 'letter'. Then there are 11 'letters' (W, O, O, LL, O, O, N, G, A, BB, A) to arrange, with four O's, two A's, and the remaining 'letters' appearing once each. Therefore the number of such arrangements is

$$\frac{11!}{4!\,2!}.$$

In order to determine the number of these for which the two A's are not adjacent, we take this total and subtract those where AA is also adjacent. For this, treat AA, BB, and LL as 'letters'. Then there are 10 'letters' to arrange, with four O's and the remaining 'letters' appearing once each. Therefore the number of arrangements with AA adjacent and BB adjacent and LL adjacent is

$$\frac{10!}{4!}.$$

Hence, the number of ways that Case 1 can occur is

$$\frac{11!}{4!\,2!} - \frac{10!}{4!}.$$

Case 2 and Case 3 have exactly the same number of occurrences as Case 1. Also note that the three cases are mutually exclusive (you cannot have both Case 1 and Case 2 occurring at the same time, for example).

So the number of arrangements of the word WOOLLOONGABBA for which exactly one of the three cases occurs is

$$3\left(\frac{11!}{4!\,2!} - \frac{10!}{4!}\right).$$

3. (a) An injective function $f : \{a, b, c\} \to \{1, 2, 3, 4, 5\}$ is determined by choosing distinct images for a, b, c. The number of choices is

$$5 \cdot 4 \cdot 3 = {}^5P_3 = 60.$$

(b) The number of surjective functions $f : \{1, 2, 3, 4, 5\} \to \{a, b, c\}$ is the total number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ minus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ which are not surjective. The former number is 3^5. A function which is not surjective must have image of size 1 or 2.

- In the first case, there are 3 such functions (one for each of the three choices for the image).
- In the latter case, first choose which 2 elements of $\{a, b, c\}$ will be in the image. There are $\binom{3}{2}$ such choices. For this fixed two-element image, the number of functions with this image is

$$2^5 - 2,$$

since there are 2^5 total functions from a 5-element set to a 2-element set, and we subtract the 2 constant ones (which fall into the first case, having image of size 1). Thus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ with an image of size 2 is

$$\binom{3}{2}(2^5 - 2) = 3 \cdot 30 = 90.$$

This means there are 93 functions which are not surjective, so the number of surjective functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ is

$$3^5 - 93 = 150.$$

§39 — Introduction to Probability

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 31 (week 11).

Problems

1. To form a committee, five people are to be chosen from a group of ten people.
   (a) How many different committees of five can be chosen?
   (b) Amongst the ten people, we have Alice, Bob, Eve and Oscar. Alice and Bob are extremely talkative during meetings, and so at most one of these two can be chosen. Eve and Oscar are inseparable, and so a committee must either contain both of them or neither of them. With these constraints, how many different five-person committees can be formed?
   (c) What is the probability that none of Alice, Bob, Eve and Oscar are on a committee, given that a random committee of five is chosen subject to the constraints in part (b)?
2. (a) How many positive two-digit integers are multiples of 3?
   (b) What is the probability that a randomly chosen positive two-digit integer is a multiple of 3?
   (c) What is the probability that a randomly chosen positive two-digit integer is a multiple of 4?

Solutions

1. (a) Number of different committees of five is

$$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252.$$

   (b) Let A, B be Alice and Bob, and let E, O be Eve and Oscar. There are 6 other people. We split into cases.

   Case 1: the committee contains both E and O. Then we choose 3 more people from the remaining 8 with the restriction that we cannot choose both A and B. There are $\binom{8}{3}$ ways to choose 3 more people from the remaining 8 to be on the committee; of these, there are $\binom{6}{1}$ ways in which both A and B are chosen (such a committee must have E, O, A, B so there is only one more person to choose from the remaining 6 people). Thus the number of committees for this case is

$$\binom{8}{3} - \binom{6}{1} = 56 - 6 = 50.$$

   Case 2: the committee contains neither E nor O. Then we choose 5 people from the remaining 8, again not allowing both A and B. There are $\binom{8}{5}$ ways to choose 5 people from the remaining 8 people to be on the committee; of these, there are $\binom{6}{3}$ ways in which both A and B are chosen. Thus the number of committees for this case is

$$\binom{8}{5} - \binom{6}{3} = 56 - 20 = 36.$$

   Hence the total number is $50 + 36 = 86$.

   (c) To have none of Alice, Bob, Eve, or Oscar on the committee, we must choose all 5 members from the other 6 people, which can be done in $\binom{6}{5} = 6$ ways. Therefore the probability is

$$\frac{6}{86} = 0.069767\ldots$$

2. (a) The positive two-digit multiples of 3 occur as every third number from 12 to 99, so there are

$$\frac{99 - 12}{3} + 1 = 30$$

such numbers.

(b) There are 90 positive two-digit integers (9 choices for the first digit and 10 choices for the second digit). Thus, by part (a), the probability that a randomly selected positive two-digit number is a multiple of 3 is

$$\frac{30}{90} = \frac{1}{3}.$$

(c) The positive two-digit multiples of 4 occur as every fourth number from 12 to 96, so there are

$$\frac{96-12}{4} + 1 = 22$$

such numbers. Hence the probability that a randomly selected positive two-digit number is a multiple of 4 is

$$\frac{22}{90} = \frac{11}{45}.$$

§40 — Binomial Coefficients

Epp 4th ed. pp. 565–591 · 5th ed. (metric) pp. 617–641. Lecture 31 (week 11).

Problems

1. What is the coefficient of x^4 in $(2+3x)^7$?
2. (a) What is the coefficient of x^{12} in $(3-x^3)^6$?
   (b) What is the coefficient of x^8 in $(3-x^3)^6$?
3. What is the coefficient of x^2 in the expansion of $(3-x)^6$?
4. What is the coefficient of x^5 in the expansion of $(2x+1)^{20}$?
5. What is the coefficient of x^5 in the expansion of $\left(3x^2 - \dfrac{2}{x}\right)^7$?

Solutions

1. By the binomial theorem,

$$(2+3x)^7 = \sum_{k=0}^{7} \binom{7}{k} 2^{7-k}(3x)^k.$$

The term x^4 appears only when $k=4$. This term is $\binom{7}{4}2^3(3x)^4$. Therefore the coefficient of x^4 is

$$\binom{7}{4}2^3 3^4 = 35 \times 8 \times 81 = 22\,680.$$

2. By the binomial theorem,

$$(3-x^3)^6 = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-x^3)^k = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-1)^k x^{3k}.$$

(a) The term involving x^{12} is $\binom{6}{4}3^2(-1)^4 x^{3\cdot 4}$, so the coefficient of x^{12} is

$$15 \times 9 \times (-1)^4 = 135.$$

(b) Every power of x that appears is a multiple of 3. Since 8 is not a multiple of 3, there is no x^8 term, so the coefficient of x^8 is $\mathbf{0}$.

3. By the binomial theorem,

$$(3-x)^6 = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-x)^i = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-1)^i x^i.$$

The term x^2 appears only when $i=2$, so the coefficient of x^2 is

$$\binom{6}{2}3^{6-2}(-1)^2 = \binom{6}{2}3^4 = 1215.$$

4. By the binomial theorem,

$$(2x+1)^{20} = \sum_{k=0}^{20} \binom{20}{k} (2x)^{20-k}(1)^k.$$

The term x^5 appears only when $k = 15$, where the term is $\binom{20}{15}(2x)^5$, so the coefficient of x^5 is

$$\binom{20}{5} 2^5 = 496\,128.$$

5. By the binomial theorem,

$$\left(3x^2 - \frac{2}{x}\right)^7 = \sum_{i=0}^{7} \binom{7}{i} (3x^2)^{7-i} \left(-\frac{2}{x}\right)^i = \sum_{i=0}^{7} \binom{7}{i} 3^{7-i}(-2)^i x^{14-3i}.$$

The term x^5 appears only when $14 - 3i = 5$, i.e. $i = 3$. Therefore the coefficient of x^5 is

$$\binom{7}{3} 3^4(-2)^3 = -22\,680.$$

§41 — Inclusion Exclusion

Epp 4th ed. pp. 545–549 · 5th ed. (metric) pp. 595–599. Lecture 32 (week 12).

Problems

1. Out of 100 people surveyed, 40 people like apples, 50 like bananas and 40 like cherries. 15 like apples and bananas, 16 like bananas and cherries, 17 like cherries and apples and 10 people like all three. How many people do not like any of the three fruits?
2. How many integers between 1 and 600 inclusive are coprime with 15? That is, how many integers n satisfy $1 \leq n \leq 600$ and $\gcd(n, 15) = 1$?
3. Seven friends, named Alice, Bob, Charlie, Delia, Edward, Fred and George, stand in a line for a photograph. How many different arrangements are there of the seven friends standing in a line such that Alice is not next to Charlie and Bob is not next to Delia?

Solutions

1. Let A be the set of people who like apples, B the set of people who like bananas, and C the set of people who like cherries. We are given

$$|A| = 40,\ |B| = 50,\ |C| = 40, \quad |A \cap B| = 15,\ |B \cap C| = 16,\ |C \cap A| = 17, \quad |A \cap B \cap C| = 10.$$

   By inclusion–exclusion,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C| \\ &= 40 + 50 + 40 - 15 - 17 - 16 + 10 \\ &= 92. \end{aligned}$$

   Hence the number of people who do not like any of the three fruits is

$$100 - |A \cup B \cup C| = 100 - 92 = 8.$$

2. Let $U = \{1, 2, \ldots, 600\}$. Define

$$A = \{n \in U : 3 \mid n\}, \qquad B = \{n \in U : 5 \mid n\}.$$

   Then n is not coprime to 15 if and only if $n \in A \cup B$. We have

$$|A| = \frac{600}{3} = 200, \qquad |B| = \frac{600}{5} = 120, \qquad |A \cap B| = \frac{600}{15} = 40.$$

   By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 200 + 120 - 40 = 280.$$

   Therefore the number of n with $\gcd(n, 15) = 1$ is

$$|U| - |A \cup B| = 600 - 280 = 320.$$

3. Let U be the set of all linear arrangements of the 7 friends, so $|U| = 7!$. Define

$$A = \{\text{arrangements in which Alice is next to Charlie}\},$$
$$B = \{\text{arrangements in which Bob is next to Delia}\}.$$

We want to count the number of arrangements in U which are neither in A nor in B. The required number is $|U \setminus (A \cup B)| = |U| - |A \cup B|$.

To count $|A|$, treat {Alice, Charlie} as a single block. There are 6! ways to arrange the 6 "objects", and for each of these there are 2 ways to order Alice and Charlie within their block (either Alice or Charlie to the left). Hence

$$|A| = 2 \cdot 6!.$$

Similarly, $|B| = 2 \cdot 6!$.

To count $|A \cap B|$, treat both pairs {Alice, Charlie} and {Bob, Delia} as two single blocks. There are 5! ways to arrange the 5 objects (two blocks plus the other three people), and for each of these there are $2 \cdot 2$ internal orders of the two blocks. Hence

$$|A \cap B| = 4 \cdot 5!.$$

By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!.$$

Therefore

$$|U \setminus (A \cup B)| = 7! - (2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!) = 2640.$$

§42 — The Pigeonhole Principle

Epp 4th ed. pp. 554–565 · 5th ed. (metric) pp. 604–616. Lecture 33 (week 12).

Problems

1. (a) Explain why, in a group of 50 people, at least five people were born in the same month.

   (b) How many people do you need to ensure that at least seven people were born in the same month?

2. Show that, if we select six distinct integers from the set $\{1, 2, \ldots, 10\}$, two of these must add to give 11.

3. A computer network consists of six computers. Each computer is directly connected to zero or more of the other computers. Show that there are at least two computers in the network that are directly connected to the same number of other computers.

4. During a month with 30 days, a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must play exactly 14 games.

5. Let $S = \{1, 2, \ldots, 100\}$. What is the minimum number of integers you must pick from S to be sure that at least one pair has a difference which is divisible by 3?

Solutions

1. (a) There are 12 months (pigeonholes) and 50 people (pigeons). If each month had at most 4 birthdays, then there would be at most $12 \cdot 4 = 48$ people. Since $50 > 48$, by the pigeonhole principle some month must contain at least 5 people.

   (b) To guarantee at least 7 people are born in the same month, note that if each month had at most 6 birthdays, then there could be at most $12 \cdot 6 = 72$ people. Therefore with **73** people, by the pigeonhole principle some month has at least 7 people. Moreover, 72 people is not enough (take 6 born in each month), so the minimum is 73.

2. Partition $A = \{1, 2, \ldots, 10\}$ into the 5 pairs

$$\{1, 10\},\ \{2, 9\},\ \{3, 8\},\ \{4, 7\},\ \{5, 6\},$$

   each summing to 11. In order for a selection of distinct integers from the set A to **not** have two that add to give 11, at most one integer can be chosen from each of the subsets. Choosing 6 distinct integers from A forces us to select two numbers from the same pair (there are 5 pairs but 6 choices), by the pigeonhole principle. Those two numbers then add to 11.

3. For each computer, let its **degree** be the number of other computers it is directly connected to. With 6 computers, each degree is an integer in $\{0, 1, 2, 3, 4, 5\}$. It is impossible to have both a computer of degree 0 and a computer of degree 5 (if one is connected to everyone, then none has degree 0). Hence the degrees must all lie in one of the two 5-element sets

$$\{0, 1, 2, 3, 4\} \quad \text{or} \quad \{1, 2, 3, 4, 5\}.$$

So, in either case, there are only 5 possible degree values available for 6 computers. By the pigeonhole principle, at least two computers have the same degree, i.e. are connected to the same number of other computers.

4. Let g_i be the total number of games played in the first i days, for $i = 1, 2, \ldots, 30$. Then

$$1 \leq g_1 < g_2 < \cdots < g_{30} \leq 45$$

because at least one game is played each day. Consider also the 30 numbers

$$g_1 + 14,\ g_2 + 14,\ \ldots,\ g_{30} + 14,$$

which satisfy $15 \leq g_1 + 14 < \cdots < g_{30} + 14 \leq 59$. Thus we have 60 integers

$$g_1, \ldots, g_{30},\ g_1 + 14, \ldots, g_{30} + 14$$

all lying in the set $\{1, 2, \ldots, 59\}$ of size 59. By the pigeonhole principle, two of these 60 integers are equal. Since the g_i are strictly increasing, no equality can occur among the g_i themselves, and likewise no equality can occur among the $g_i + 14$ themselves. Therefore we must have

$$g_j = g_i + 14$$

for some $i, j \in \{1, \ldots, 30\}$. Then the number of games played from day $i + 1$ through day j is

$$g_j - g_i = 14,$$

so there is a period of consecutive days during which exactly 14 games are played.

5. First, we note that two integers have a difference that is divisible by 3 if and only if they are congruent modulo 3 (have the same remainder when divided by 3). Now, the set S can be partitioned into three sets based on their congruence class modulo 3. By the pigeonhole principle, if we select **4** numbers from S, at least two of them must belong to the same congruence class. These two will have difference that is divisible by 3. Note that 4 is the minimum number of selections that guarantees this, since it is possible to select 3 numbers where no two of them have difference divisible by 3 (select one from each congruence class).

§43 — Introduction to Graph Theory

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 33 (week 12).

Problems

1. For each of the following, state whether or not there exists a simple graph with the stated number of vertices and degrees. Draw the graph, or explain why one does not exist.
   (a) Five vertices with degrees 3, 3, 2, 2, 2.
   (b) Seven vertices with degrees 4, 2, 3, 1, 1, 1, 1.
   (c) Five vertices with degrees 5, 4, 3, 1, 1.
2. A graph has 10 edges and 6 vertices. Five of the vertices have degree 3. What is the degree of the remaining vertex?
3. Let n be a positive integer and let K_n be the complete graph with n vertices. How many edges does K_n have?
4. A graph has 27 edges and every vertex has degree 2, 3 or 4. If there are 7 vertices that have degree 4 and 4 vertices that have degree 3, then how many vertices of degree 2 are there?

Solutions

1. (a) **Yes**, such a simple graph exists. One drawing has vertices a, b, c, d, e and the six edges

$$ab, \quad ac, \quad ad, \quad bc, \quad be, \quad de,$$

giving $\deg(a) = 3$, $\deg(b) = 3$, $\deg(c) = 2$, $\deg(d) = 2$, $\deg(e) = 2$ as required.

   (b) **No** such graph exists. If the degrees are 4, 2, 3, 1, 1, 1, 1, then the sum of degrees is

$$4 + 2 + 3 + 1 + 1 + 1 + 1 = 13,$$

which is odd. Remember (by the Handshake Theorem) that the sum of the degrees in any graph equals twice the number of edges, and so is always even. So such a graph cannot exist.

(c) **No** such graph exists. In a simple graph on 5 vertices, the largest possible degree is 4, but the sequence contains a vertex of degree 5, which is impossible. So there is no such simple graph.

2. Since the graph has 10 edges, the sum of all the degrees is $2 \cdot 10 = 20$. If five vertices have degree 3, the sum of their degrees is $5 \cdot 3 = 15$, so the remaining vertex has degree

$$20 - 15 = 5.$$

3. In K_n, an edge is determined by choosing 2 distinct vertices, so the number of edges is

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

4. Let x be the number of vertices of degree 2. Since the graph has 27 edges, the sum of degrees is $2 \cdot 27 = 54$. Given that there are seven vertices of degree 4 and four vertices of degree 3, and all other vertices have degree 2, we have

$$2x + 4 \cdot 7 + 3 \cdot 4 = 54.$$

This means $x = 7$.

§44 — Walks, Trails and Circuits

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 34 (week 12).

Problems

1. Let G and H be the graphs below.

   G has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is drawn with a **loop at** v_2, a **loop at** v_5, and **two parallel edges between** v_1 **and** v_2. Its degree sequence is

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   so G is connected with 10 edges.

   H has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is a simple connected graph drawn as the 4-cycle $v_1v_2v_3v_4v_1$ with a single pendant edge v_3v_5, giving degrees

   $$\deg(v_1) = 2, \quad \deg(v_2) = 2, \quad \deg(v_3) = 3, \quad \deg(v_4) = 2, \quad \deg(v_5) = 1.$$

   For each of the following statements, explain why it is true or false.

   (a) G is a simple graph.

   (b) The sum of the degrees of the vertices of G is 18.

   (c) G contains an Euler circuit.

   (d) H contains an Euler trail.

2. Does the following graph contain an Euler circuit? (The graph shown is connected and has exactly two vertices of degree 3.)

3. Let G be a simple, connected, Eulerian graph with eight vertices and let e be the number of edges in G. Prove that $8 \leq e \leq 24$.

Solutions

1. (a) This statement is **false**. The graph G has loops (at v_2 and v_5) and it also has multiple edges between v_1 and v_2, so G is not simple.

   (b) This statement is **false**. A loop contributes 2 to the degree, so we have

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   and thus the sum of the degrees is $4 + 6 + 4 + 2 + 4 = 20 \neq 18$.

   (c) This statement is **true**. The graph G is connected and every vertex has even degree (as computed above), so G contains an Euler circuit.

(d) This statement is **true**. In H, the degrees are

$$\deg(v_1) = 2,\ \deg(v_2) = 2,\ \deg(v_4) = 2,\ \deg(v_3) = 3,\ \deg(v_5) = 1,$$

so exactly two vertices have odd degree (namely v_3 and v_5). Therefore H has an Euler trail (starting at one of v_3, v_5 and ending at the other).

2. **No.** The graph is connected, but has two vertices of degree 3, so not all vertices have even degree. Hence there is no Euler circuit.

3. Since G is connected and Eulerian, every vertex has even degree, and (because G is simple and connected with 8 vertices) each vertex has degree at least 2. Hence

$$2e = \sum_{v} \deg(v) \geq 8 \cdot 2 = 16,$$

so $e \geq 8$. Moreover, in a simple graph on 8 vertices we have $\deg(v) \leq 7$, and because G is Eulerian all degrees are even, so in fact $\deg(v) \leq 6$ for every vertex. Therefore

$$2e = \sum_{v} \deg(v) \leq 8 \cdot 6 = 48,$$

so $e \leq 24$. Hence $8 \leq e \leq 24$. □

§45 — Matrix Representations of Graphs

Epp 4th ed. pp. 661–675 · 5th ed. (metric) pp. 698–712. Lecture 35 (week 13).

Problems

1. Let G be the graph with vertex set $\{v_1, v_2, v_3, v_4\}$ and edge set $\{a, b, c, d, e, f\}$, where the edges are

edge	endpoints
a	$v_1 v_2$
b	$v_2 v_3$
c	$v_2 v_3$ (parallel to b)
d	$v_3 v_4$
e	$v_2 v_4$
f	loop at v_4

(a) Write down an adjacency matrix for G. Make sure you clearly label the rows and columns of your matrix.

(b) Write down an incidence matrix for G. Make sure you clearly label the rows and columns of your matrix.

(c) Does G have an Euler circuit? If yes, write it out as a sequence of vertices and edges. If not, determine the fewest number of edges that would need to be added to G to create a new graph that does have an Euler circuit.

2. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 3 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 3 & 0 & 1 & 1 & 0 \end{pmatrix}$$

(a) Draw the graph G.

(b) Explain whether or not G has an Euler circuit or an Euler trail.

3. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Explain whether or not G is Eulerian.

Solutions

1. (a) The labelled adjacency matrix for G is

	v_1	v_2	v_3	v_4
$\mathbf{v_1}$	0	1	0	0
$\mathbf{v_2}$	1	0	2	1
$\mathbf{v_3}$	0	2	0	1
$\mathbf{v_4}$	0	1	1	1

(where the entry 1 on the diagonal at v_4 records the single loop at v_4).

(b) The labelled incidence matrix for G is

	a	b	c	d	e	f
$\mathbf{v_1}$	1	0	0	0	0	0
$\mathbf{v_2}$	1	1	1	0	1	0
$\mathbf{v_3}$	0	1	1	1	0	0
$\mathbf{v_4}$	0	0	0	1	1	2

(where the entry 2 in the bottom right indicates the loop that is incident twice with v_4).

(c) The degrees are

$$\deg(v_1) = 1, \quad \deg(v_2) = 4, \quad \deg(v_3) = 3, \quad \deg(v_4) = 4,$$

so G does **not** have an Euler circuit (since v_1 and v_3 have odd degree).

The fewest edges to add to make all degrees even is **1**; for example, adding an edge g between vertices v_1 and v_3 creates a new connected graph in which all of the vertices have even degree.

An example of an Euler circuit in the new graph is

$$v_1,\ a,\ v_2,\ b,\ v_3,\ d,\ v_4,\ f,\ v_4,\ e,\ v_2,\ c,\ v_3,\ g,\ v_1.$$

2. (a) Reading the matrix off (with vertices $v_1, \ldots, v_5$ in matrix order), G has the edges

- v_1v_2 — a single edge,
- v_1v_5 — **three** parallel edges,
- v_2v_3 — **two** parallel edges,
- v_3v_4 — a single edge,
- v_3v_5 — a single edge,
- v_4v_5 — a single edge.

(b) The degrees are

$$\deg(v_1) = 4,\ \deg(v_2) = 3,\ \deg(v_3) = 4,\ \deg(v_4) = 2,\ \deg(v_5) = 5,$$

so there is **no Euler circuit** (since v_2 and v_5 have odd degree), but there **is an Euler trail** (exactly two odd-degree vertices) from v_2 to v_5.

3. Let the vertices be $v_1, v_2, v_3, v_4, v_5, v_6$ in the order of the matrix. Reading the matrix off, G has edges

$$v_1v_2, \quad v_1v_4, \quad v_2v_4, \quad v_3v_5, \quad v_3v_6, \quad v_5v_6,$$

that is, two disjoint triangles: one on $\{v_1, v_2, v_4\}$ and one on $\{v_3, v_5, v_6\}$.

The graph is **not connected** (e.g. there is no walk from vertex v_1 to vertex v_3). Hence G is not Eulerian.

(Errata note: the source document's solution to 1(b) was corrected on 11 August 2026 — the note in brackets had previously copied the note from 1(a). The corrected note is the one given above.)

§46 — Trees

Epp 4th ed. pp. 683–701 · 5th ed. (metric) pp. 720–742. Lecture 36 (week 13).

Problems

1. A tree has 11 vertices, of which exactly four vertices have degree 1 and exactly one vertex has degree 4. Determine the degrees of the remaining six vertices.
2. Let T be a tree with p vertices, where $p \geq 11$. Suppose T has precisely six vertices of degree 1 and precisely four vertices of degree 3. Determine the degree of each of the remaining $p - 10$ vertices of T.
3. Let T be a tree on 12 vertices. Suppose T has exactly three vertices of degree 3 and each of the remaining vertices has degree 1 or 5. Using theorems that were given in lectures, determine the number of vertices of degree 5.
4. Two trees with the same vertex set $\{1, 2, \ldots, n\}$ are **distinct** if their edge sets are not equal. Use mathematical induction to prove that for each integer $n \geq 2$, the number of distinct trees with vertex set $\{1, 2, \ldots, n\}$ is at least $(n-1)!$.

Solutions

1. A tree with 11 vertices has $e = 10$ edges, so by the Handshake Theorem, the sum of degrees is $2e = 20$. We are given that exactly four vertices have degree 1 and exactly one vertex has degree 4. Let $v_1, v_2, \ldots, v_6$ be the remaining vertices whose degrees are to be determined. We have

$$\sum_{i=1}^{6} \deg(v_i) + 4 \cdot 1 + 1 \cdot 4 = 20$$

$$\sum_{i=1}^{6} \deg(v_i) = 12.$$

None of these six vertices $v_1, v_2, \ldots, v_6$ can have degree 1 (since there are exactly four vertices of degree 1, already accounted for). Hence each has degree at least 2. Because six vertices of degree at least 2 have total degree 12, each must have degree exactly 2.

Thus the remaining six vertices all have **degree 2**.

2. T is a tree with p vertices and so must have $p-1$ edges. Now by the Handshake Theorem we know

$$2(p-1) = \sum_{i=1}^{p} \deg(v_i).$$

Using the known degrees we can write this as

$$\begin{aligned} 2(p-1) &= 6 \cdot 1 + 4 \cdot 3 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-1) &= 18 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2p - 2 - 18 &= \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-10) &= \sum_{i=1}^{p-10} \deg(v_i). \end{aligned}$$

Rewriting the final line as

$$\frac{\sum_{i=1}^{p-10} \deg(v_i)}{p-10} = 2, \qquad \text{i.e.} \qquad \frac{\deg(v_1) + \deg(v_2) + \cdots + \deg(v_{p-10})}{p-10} = 2,$$

we see that the average degree of the remaining $p-10$ vertices is 2. However, we know that there are no more vertices of degree 1. Thus each of the remaining $p-10$ vertices must have **degree exactly 2**.

3. Let x be the number of vertices of degree 5 and y the number of vertices of degree 1. Then, because the tree has 12 vertices, we have

$$x + y + 3 = 12.$$

This simplifies to give $x + y = 9$.

Now, since T is a tree on 12 vertices, it must have $e = 11$ edges. By the Handshake Theorem, the sum of degrees is $2e = 22$, so

$$3 \cdot 3 + 5x + 1 \cdot y = 22.$$

This simplifies to give $5x + y = 13$.

Subtracting $x + y = 9$ from $5x + y = 13$ gives $4x = 4$, hence $x = 1$. Therefore there is exactly **one** vertex of degree 5.

4. We prove by induction that the number of distinct trees with vertex set $\{1, 2, \dots, n\}$ is at least $(n-1)!$.

Basis: let $n = 2$. Here $(n-1)! = (2-1)! = 1$. There is exactly one tree on $\{1, 2\}$, namely the single edge $\{1, 2\}$. So the base case is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and there are at least $(k-1)!$ distinct trees on $\{1, 2, \dots, k\}$.

Now consider $n = k + 1$. We aim to show that there are at least $k!$ distinct trees on vertex set $\{1, 2, \dots, k, k+1\}$.

Let T be a tree on vertex set $\{1, 2, \dots, k\}$. For any choice of $m \in \{1, 2, \dots, k\}$, we form a graph T_m on vertex set $\{1, 2, \dots, k, k+1\}$ as follows: start with tree T, add a new vertex $k+1$, and the edge $\{k+1, m\}$.

Note that T_m is connected (since $k+1$ is joined to m, and T was connected). Also, T_m has no circuit because T is a tree and adding a new leaf does not create a circuit. Thus T_m is a tree. Moreover, different choices of m give rise to distinct trees T_m, because their edge sets are different.

By the inductive hypothesis, there are at least $(k-1)!$ choices for the tree T. Since there are k choices for the vertex m, there are at least $k \cdot (k-1)! = k!$ trees T_m on vertex set $\{1, 2, \dots, k+1\}$.

By the principle of mathematical induction, this completes the proof. $\square$

See also

- math1061[368] — assessment weights and the full lecture schedule
- Logic: logical-connectives[369] · logical-equivalence-laws[370] · conditional-statements[371] · valid-argument-forms[372] · determining-argument-validity[373] · quantified-statements[374]
- Number theory and proof: proof-techniques[375] · rational-and-irrational-numbers[376] · divisibility-and-factorisation[377] · modular-arithmetic[378] · gcd-lcm-and-euclidean-algorithm[379]
- Graph theory (§43–§46): graphs[380] · walks-trails-and-circuits[381] · euler-circuits-and-trails[382] · adjacency-matrices[383] · incidence-matrices[384] · trees[385]

Rational & Irrational Numbers

The definitions and closure results that make $\mathbb{Q}$ a workable object in proofs, plus the classic irrationality argument.

Definitions

$$r \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z} \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0$$

$$r \in \overline{\mathbb{Q}} \iff r \notin \mathbb{Q}$$

$\overline{\mathbb{Q}} = \mathbb{R} \setminus \mathbb{Q}$ is the set of **irrational** numbers. The barred symbol is what this course writes, not $\mathbb{R} \setminus \mathbb{Q}$. Figure 44 shows how the four sets sit together.

[368] courses/math1061/math1061.pdf
[369] courses/math1061/logical-connectives.pdf
[370] courses/math1061/logical-equivalence-laws.pdf
[371] courses/math1061/conditional-statements.pdf
[372] courses/math1061/valid-argument-forms.pdf
[373] courses/math1061/determining-argument-validity.pdf
[374] courses/math1061/quantified-statements.pdf
[375] courses/math1061/proof-techniques.pdf
[376] courses/math1061/rational-and-irrational-numbers.pdf
[377] courses/math1061/divisibility-and-factorisation.pdf
[378] courses/math1061/modular-arithmetic.pdf
[379] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[380] courses/math1061/graphs.pdf
[381] courses/math1061/walks-trails-and-circuits.pdf
[382] courses/math1061/euler-circuits-and-trails.pdf
[383] courses/math1061/adjacency-matrices.pdf
[384] courses/math1061/incidence-matrices.pdf
[385] courses/math1061/trees.pdf

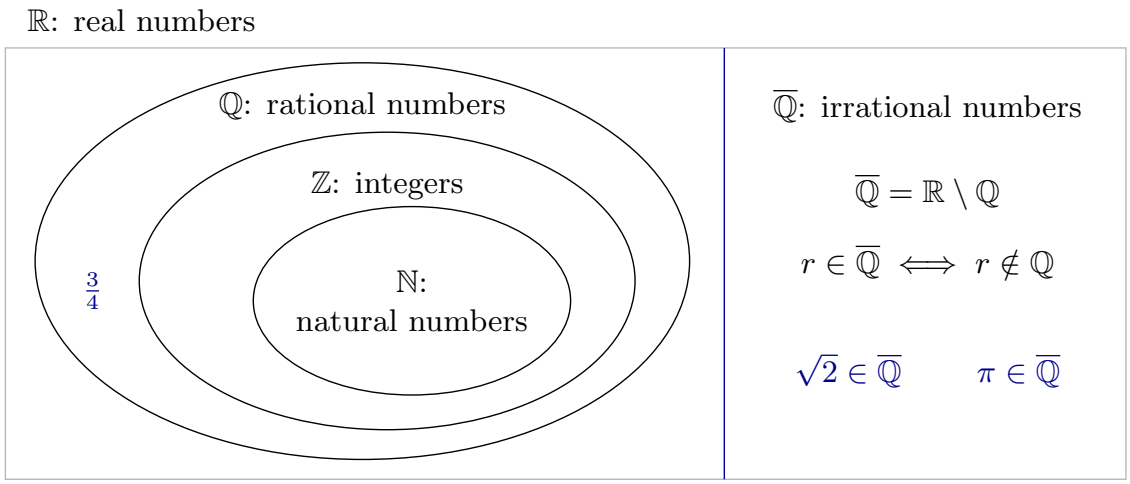


Figure 44: The number systems as nested closed curves with each name written inside its own region, and the irrationals in their own panel because they are the part of the reals that is left over rather than a set that contains any of the others. The three examples are in blue. Two things to read off it — every integer is rational (it is n/1), and no number is in both panels, which is exactly what the definition of the bar says. The course leaves open whether N contains 0, so nothing here should be read as settling that.

Note the definition is existential: to show r is rational you must **exhibit** integers a and b with $b \neq 0$. Nearly every proof below ends by checking three things — the numerator is an integer, the denominator is an integer, and the denominator is non-zero.

Fact: every rational number can be written as a fraction in **lowest terms** (numerator and denominator have no common factors).

Why irrationality statements want contradiction or contraposition

"r is irrational" is a *negative* statement — $r \notin \mathbb{Q}$ — so a direct proof has nothing to unfold. Assuming the negation instead ($r \in \mathbb{Q}$) hands you $r = \frac{a}{b}$ to work with. See proof-techniques[386] for the general shape, and the collected verdicts in 2026-08-13-proof-by-contraposition[387] for which method works on each statement.

Concretely, for **the sum of any rational number and any irrational number is irrational**:

- Symbolically: $\forall r, s \in \mathbb{R}$, if $r \in \mathbb{Q}$ and $s \in \overline{\mathbb{Q}}$ then $r + s \in \overline{\mathbb{Q}}$ — or equivalently $\forall r \in \mathbb{Q}$ and $\forall s \in \mathbb{R}$, if $s \in \overline{\mathbb{Q}}$ then $r + s \in \overline{\mathbb{Q}}$.
- **Direct proof**: suppose $r \in \mathbb{Q}$ and $s \in \overline{\mathbb{Q}}$ — and now you're stuck, because $s \in \overline{\mathbb{Q}}$ gives you nothing to substitute.
- **Contradiction**: suppose $\exists r \in \mathbb{Q}, s \in \mathbb{R}$ with $s \in \overline{\mathbb{Q}}$ and $r + s \in \mathbb{Q}$.
- **Contraposition**: prove $\forall r \in \mathbb{Q}$ and $\forall s \in \mathbb{R}$, if $r + s \in \mathbb{Q}$ then $s \in \mathbb{Q}$.

  Proof by contraposition. Suppose $r \in \mathbb{Q}$, $s \in \mathbb{R}$ and $r + s \in \mathbb{Q}$. Since $r \in \mathbb{Q}$, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Since $r + s \in \mathbb{Q}$, $r + s = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ with $d \neq 0$. Now

  $$s = (r + s) - r = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}.$$

  Since $a, b, c, d \in \mathbb{Z}$ we know $bc - ad \in \mathbb{Z}$ and $bd \in \mathbb{Z}$; and $bd \neq 0$ since $b \neq 0$ and $d \neq 0$. Thus $s \in \mathbb{Q}$. $\square$

The trick that makes it work is writing the thing you want in terms of the things you have: $s = (r + s) - r$. The second fraction needs a **fresh pair of variables** c, d — nothing relates it to a, b, and reusing them is one of the standard errors in proof-techniques[388].

[386] courses/math1061/proof-techniques.pdf
[387] courses/math1061/2026-08-13-proof-by-contraposition.pdf
[388] courses/math1061/proof-techniques.pdf

Closure results

$\forall r \in \mathbb{Q}, (2r^2 - 3r + 1) \in \mathbb{Q}$ — direct proof is best here; contraposition gets stuck.

> Let $r \in \mathbb{Q}$, so $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Then
>
> $$2r^2 - 3r + 1 = \frac{2a^2}{b^2} - \frac{3ab}{b^2} + \frac{b^2}{b^2} = \frac{2a^2 - 3ab + b^2}{b^2}.$$
>
> Since $a, b \in \mathbb{Z}$ we have $2a^2 - 3ab + b^2 \in \mathbb{Z}$ and $b^2 \in \mathbb{Z}$, and $b^2 \neq 0$ since $b \neq 0$. So $2r^2 - 3r + 1 \in \mathbb{Q}$. □

$\forall r \in \mathbb{R}$, **if r^2 is irrational then r is irrational.** Proved by contraposition in proof-techniques[389] — the contrapositive is "if $r \in \mathbb{Q}$ then $r^2 \in \mathbb{Q}$", i.e. $r^2 = \frac{a^2}{b^2}$ with $a^2, b^2 \in \mathbb{Z}$ and $b^2 \neq 0$.

For real m, n: if m is irrational and n is rational, then $m - n$ is irrational.

> *Proof by contradiction.* Suppose m is irrational, n is rational, but $m - n$ is rational. Then $n = \frac{a}{b}$ and $m - n = \frac{c}{d}$ for integers a, b, c, d with $b, d \neq 0$. Since $m = (m - n) + n$,
>
> $$m = \frac{c}{d} + \frac{a}{b} = \frac{bc + ad}{bd},$$
>
> with $bc + ad \in \mathbb{Z}$, $bd \in \mathbb{Z}$ and $bd \neq 0$. So m is rational, contradicting the assumption. □

For a real number r: if $2r^2 - 3r$ is irrational, then r is irrational.

> *Proof by contraposition.* The contrapositive is: if $r \in \mathbb{Q}$ then $2r^2 - 3r \in \mathbb{Q}$. Let $r = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$. Then $2r^2 - 3r = \frac{2a^2 - 3ab}{b^2}$, with integer numerator and non-zero integer denominator. □

For all real r, s and n: if r is irrational, s is rational and n is a positive integer, then $n(r - s)$ is irrational.

> *Proof by contradiction.* Suppose otherwise: $r \in \overline{\mathbb{Q}}$, $s \in \mathbb{Q}$, $n \in \mathbb{Z}^+$, but $n(r - s) \in \mathbb{Q}$. Write $s = \frac{a}{b}$ and $n(r - s) = \frac{c}{d}$ with $b, d \neq 0$. Since $n \neq 0$,
>
> $$r = s + \frac{c}{d} \cdot \frac{1}{n} = \frac{a}{b} + \frac{c}{dn} = \frac{adn + bc}{bdn}.$$
>
> Here $adn + bc \in \mathbb{Z}$, $bdn \in \mathbb{Z}$, and $bdn \neq 0$ since b, d, n are all non-zero. So $r \in \mathbb{Q}$ — a contradiction. □

For every rational r, if $r \neq 0$ then $r\sqrt{2}$ is irrational. Negation: $\exists r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$.

[389] courses/math1061/proof-techniques.pdf

Proof by contradiction. Suppose the negation holds. Since $r \in \mathbb{Q}$, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and $a \neq 0$ because $r \neq 0$. Since $r\sqrt{2} \in \mathbb{Q}$, $r\sqrt{2} = \frac{c}{d}$ for integers c, d with $d \neq 0$. Then

$$\sqrt{2} = \frac{r\sqrt{2}}{r} = \frac{c}{d} \cdot \frac{b}{a} = \frac{bc}{ad},$$

where $bc \in \mathbb{Z}$, $ad \in \mathbb{Z}$ and $ad \neq 0$ (since $a \neq 0$ and $d \neq 0$). So $\sqrt{2} \in \mathbb{Q}$ — contradicting the theorem below. □

$\sqrt{2}$ is irrational

The set-up needs two ingredients: the lowest-terms fact above, and the lemma **for all integers n, if n^2 is even then n is even** (proved by contraposition — see proof-techniques[390]).

Proof by contradiction. Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and we may assume $\frac{a}{b}$ is in lowest terms.

Squaring, $2 = \frac{a^2}{b^2}$, so $a^2 = 2b^2$ and thus a^2 is even. By the lemma, a is even, so $a = 2\ell$ for some $\ell \in \mathbb{Z}$.

Substituting: $2b^2 = a^2 = (2\ell)^2 = 4\ell^2$, so $b^2 = 2\ell^2$ and b^2 is even. By the lemma again, b is even.

But now a and b are both even, so they share the common factor 2 — contradicting the assumption that $\frac{a}{b}$ is in lowest terms. Therefore $\sqrt{2} \in \overline{\mathbb{Q}}$. □

The shape of the argument is easier to hold onto than its algebra (Figure 45).

Neither a direct proof nor a contraposition proof gets off the ground here: the statement isn't a conditional with a usable hypothesis, so contradiction is the only one of the three that has anywhere to start.

See also

- proof-techniques[391] — direct / counterexample / contradiction / contraposition
- 2026-08-13-proof-by-contraposition[392] — Lecture 9
- quantified-statements[393]
- divisibility-and-factorisation[394]
- practice-problems[395] — §12 Rational Numbers, with full worked solutions

[390] courses/math1061/proof-techniques.pdf
[391] courses/math1061/proof-techniques.pdf
[392] courses/math1061/2026-08-13-proof-by-contraposition.pdf
[393] courses/math1061/quantified-statements.pdf
[394] courses/math1061/divisibility-and-factorisation.pdf
[395] courses/math1061/practice-problems.pdf

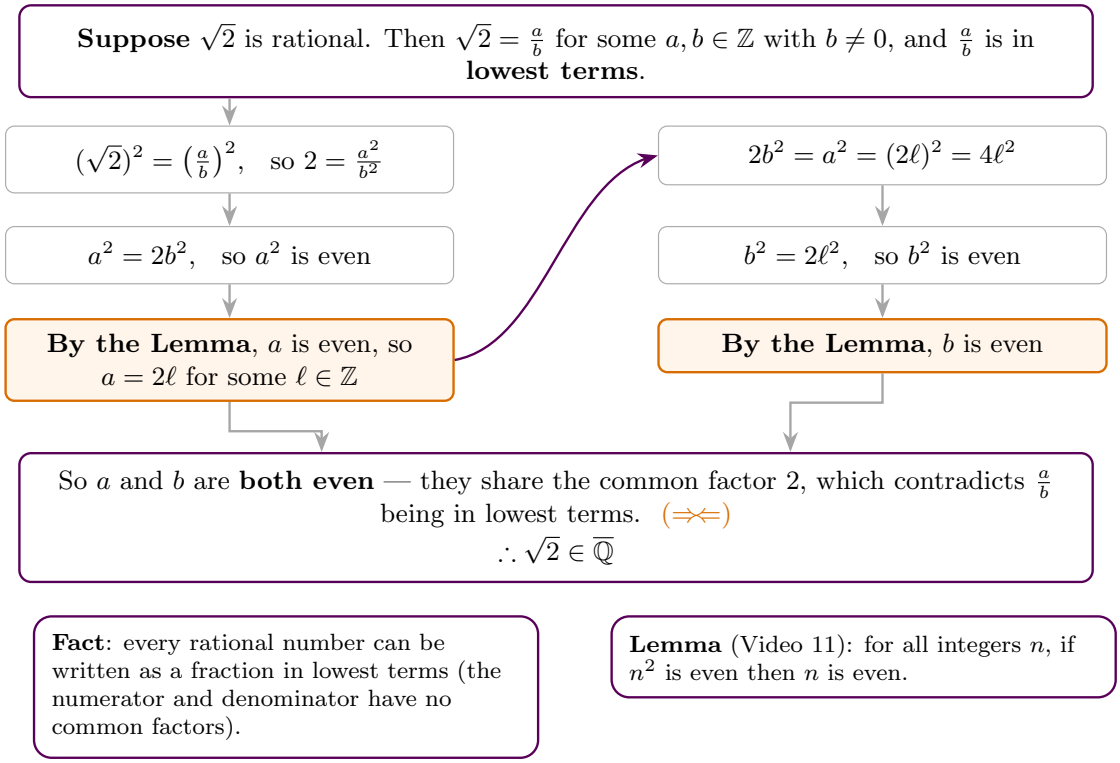


Figure 45: The same proof as a structure. It runs in two halves that use the lemma once each (orange): the left half squeezes 'a is even' out of the assumption, and the substitution a = 2l feeds the right half, which gets 'b is even'. Neither half is a contradiction on its own — the contradiction only appears when both land together and the fraction turns out not to have been in lowest terms after all. That is why the lowest-terms assumption has to be made in the very first line: it is the thing the two halves eventually collide with. The two boxes at the bottom state the Fact and the Lemma.

Reflexive, Symmetric and Transitive Relations

The three properties a relation on a single set can have, what each looks like in an arrow diagram, and how to prove or disprove each one. Relations themselves are defined in relations-on-sets[396]. The lecture is 2026-09-17-relations-reflexivity-symmetry-transitivity[397].

The definitions

A relation ρ on a set A is

(1) reflexive if and only if $\forall x \in A,\ x\ \rho\ x$.

(2) symmetric if and only if $\forall x, y \in A,\ x\ \rho\ y \to y\ \rho\ x$.

(3) transitive if and only if $\forall x, y, z \in A,\ (x\ \rho\ y \text{ and } y\ \rho\ z) \to x\ \rho\ z$.

In the arrow diagram:

- **reflexive** — every dot has a loop;
- **symmetric** — every arrow has a return arrow;
- **transitive** — every path of two arrows has a direct arrow from its start to its end, the **short cut**.

A relation fails a property when the diagram contains one of the patterns in Figure 46. Each is a **witness** — one specific element, pair or triple. Nothing more is needed to disprove a "for all".

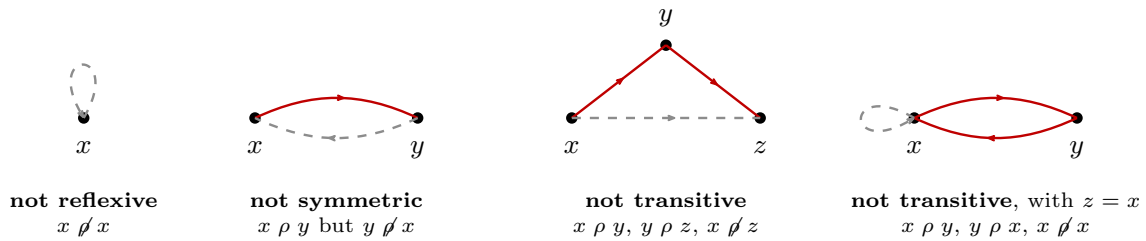
Reading the definitions carefully

Reflexive is about every element. "$\forall x \in A$" means a single element without a loop is enough to make a relation not reflexive, even if every other element has one. Disjointness, $X\ \rho\ Y \leftrightarrow X \cap Y = \emptyset$ on $\mathcal{P}(\mathbb{Z}^+)$, is *not* reflexive, though $\emptyset\ \rho\ \emptyset$ holds.

Symmetric and transitive are conditional. They say what must happen **if** certain arrows are present. Where those arrows are absent, the condition holds automatically, by vacuous truth (conditional-statements[398]). This is why a relation with very few arrows can be symmetric and transitive. The empty relation on any set is both, and so is $\{(1,1)\}$ on $\{1,2\}$.

x, y, z need not be different. In the transitive condition, z may equal x. Then it reads: if $x\ \rho\ y$ and $y\ \rho\ x$, then $x\ \rho\ x$. **In a transitive relation, any two elements related both**

[396] courses/math1061/relations-on-sets.pdf
[397] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf
[398] courses/math1061/conditional-statements.pdf



not reflexive
$x \not\rho x$

not symmetric
$x \rho y$ but $y \not\rho x$

not transitive
$x \rho y$, $y \rho z$, $x \not\rho z$

not transitive, with $z = x$
$x \rho y$, $y \rho x$, $x \not\rho x$

Figure 46: What a failure of each property looks like; any one such pattern in a diagram disproves the property. Not reflexive: one element without a loop. Not symmetric: one arrow whose return is missing. Not transitive: one path of two arrows whose short cut is missing. The fourth panel is the not-transitive pattern with $z = x$: a round trip $x \to y \to x$ needs the short cut $x \to x$, a loop, so two elements joined both ways but without loops already break transitivity. The missing arrows are dashed.

ways both have loops. Three of the transitivity counterexamples in 2026-09-17-relations-reflexivity-symmetry-transitivity[399] use exactly this: $\{1\}$ and $\{2\}$ are disjoint both ways but $\{1\}$ is not disjoint from itself; in Diagram 1 $b \to a \to b$ exists but the loop at b does not; and for $xy \equiv 1 \pmod 7$, $2 \to 4 \to 2$ exists but $2 \not\rho 2$.

Proving and disproving

Each property is a universal statement, so proving it needs a general argument about arbitrary elements, while disproving it needs one witness (quantified-statements[400], proof-techniques[401]):

	To prove it	To disprove it
reflexive	Let $x \in A$. Show $x \rho x$.	Find one $x \in A$ with $x \not\rho x$.
symmetric	Let $x, y \in A$ and suppose $x \rho y$. Show $y \rho x$.	Find $x, y \in A$ with $x \rho y$ but $y \not\rho x$.
transitive	Let $x, y, z \in A$ and suppose $x \rho y$ and $y \rho z$. Show $x \rho z$.	Find $x, y, z \in A$ with $x \rho y$ and $y \rho z$ but $x \not\rho z$.

In every proof, **unfold the definition of** ρ — turn $x \rho y$ into the condition it stands for, work with that, and fold it back up at the end. For a disproof, give specific elements and check each of the stated facts about them.

[399] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf
[400] courses/math1061/quantified-statements.pdf
[401] courses/math1061/proof-techniques.pdf

Worked: $m \rho n \leftrightarrow 6 \mid (m-n)$ **on** $\mathbb{Z}$

All three hold. Unfold with the definition of divides (divisibility-and-factorisation[402]): $m \rho n$ means $m - n = 6k$ for some $k \in \mathbb{Z}$.

- **Reflexive.** Let $m \in \mathbb{Z}$. Then $m - m = 0 = 6 \cdot 0$, so $6 \mid (m-m)$ and $m \rho m$.
- **Symmetric.** Let $m, n \in \mathbb{Z}$ with $m \rho n$, so $m - n = 6k$ for some $k \in \mathbb{Z}$. Then $n - m = 6(-k)$ and $-k \in \mathbb{Z}$, so $6 \mid (n-m)$ and $n \rho m$.
- **Transitive.** Let $m, n, p \in \mathbb{Z}$ with $m \rho n$ and $n \rho p$, so $m - n = 6k$ and $n - p = 6\ell$ for some $k, \ell \in \mathbb{Z}$. Adding, $m - p = 6(k + \ell)$ with $k + \ell \in \mathbb{Z}$, so $m \rho p$.

Its diagram on $\{0, \dots, 11\}$ is drawn in relations-on-sets[403]. The second divisibility gets a **new variable** ℓ: reusing k would claim that $m - n$ and $n - p$ are the same multiple of 6.

Worked: $x \rho y \leftrightarrow x > y$ **on** $\mathbb{Z}$

- **Not reflexive.** $0 > 0$ is false, so $0 \not\rho 0$.
- **Not symmetric.** $1 \rho 0$ since $1 > 0$, but $0 \not\rho 1$ since $0 > 1$ is false.
- **Transitive.** Suppose $x > y$ and $y > z$. Then $x > z$, so $x \rho z$.

Worked: divides, on $\{1, 2, \dots, 6\}$

$x \rho y \leftrightarrow x \mid y$ is reflexive ($x = x \cdot 1$), not symmetric ($1 \mid 2$ but $2 \nmid 1$), and transitive: if $y = xk$ and $z = y\ell$ then $z = x(k\ell)$. The diagram shows all three at once.

Checking a finite relation from its diagram

For a relation given as a diagram or a list of pairs:

1. **Reflexive:** look for a loop at every element. Any element without one is the witness.
2. **Symmetric:** for each non-loop arrow, look for its return. Any arrow without one is the witness.
3. **Transitive:** for each arrow $x \to y$, look at every arrow leaving y, say $y \to z$, and check that $x \to z$ is there. Include the paths that come back, $x \to y \to x$, whose short cut is a loop. This is the slow check, and the round trips are where it usually goes wrong.

The same procedure answers "what must be added to make it reflexive, symmetric, transitive": the missing loops, the missing returns, and the missing short cuts. For transitivity, keep checking after adding, because a new arrow can create new two-step paths. This is worked on Diagram 1 in 2026-09-17-relations-reflexivity-symmetry-transitivity[404].

[402] courses/math1061/divisibility-and-factorisation.pdf
[403] courses/math1061/relations-on-sets.pdf
[404] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf

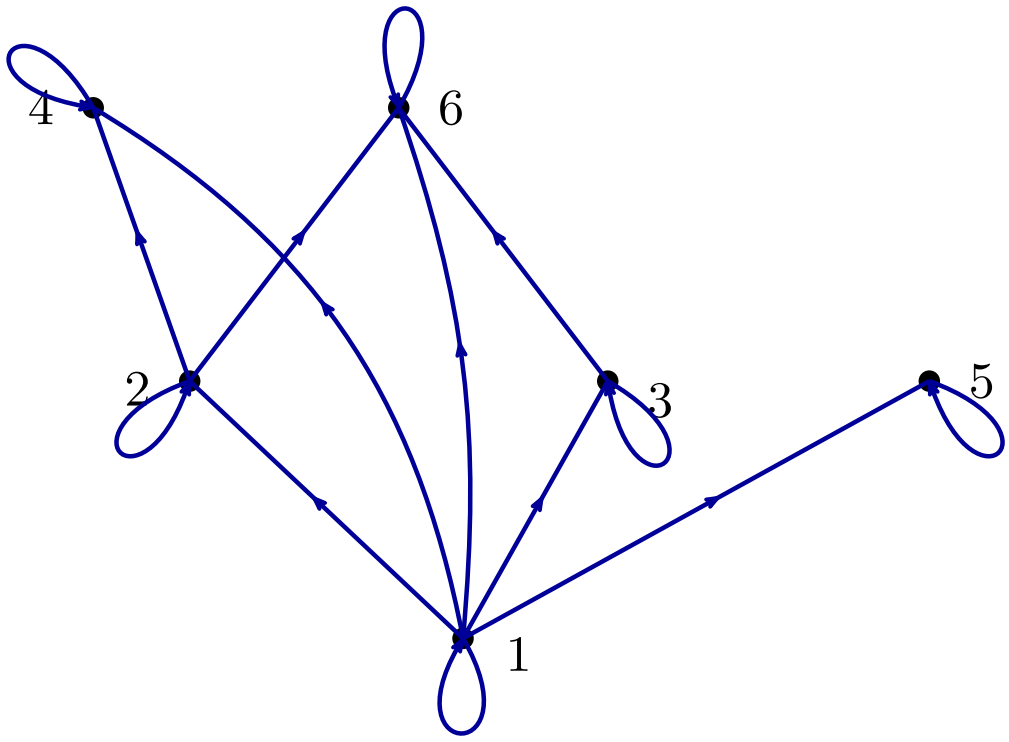


Figure 47: The relation $x \mid y$ on $1, 2, \ldots, 6$, with the numbers placed so every arrow points upward. Reflexive: a loop at every number, since each number divides itself. Not symmetric: no arrow comes back down — $1 \mid 2$, but $2 \nmid 1$. Transitive: every two-step path has its short cut, such as $1 \to 2 \to 4$ with the direct arrow $1 \to 4$. There are 14 arrows: 6 loops and 8 others.

The examples side by side

Relation	on	Reflexive	Symmetric	Transitive
$X \subset Y$ (proper subset)	$\mathcal{P}(\{1,2,3\})$	no	no	**yes**
$X \cap Y = \emptyset$	$\mathcal{P}(\mathbb{Z}^+)$	no	**yes**	no
Diagram 1	$\{a,b,c,d\}$	no	no	no
$xy \equiv 1 \pmod 7$	$\{0,\dots,6\}$	no	**yes**	no
$\{(1,1)\}$	$\{1,2\}$	no	**yes**	**yes**
$6 \mid (m-n)$	$\mathbb{Z}$	**yes**	**yes**	**yes**
$x > y$	$\mathbb{Z}$	no	no	**yes**
$x \mid y$	$\{1,\dots,6\}$	**yes**	no	**yes**

The first five are worked in 2026-09-17-relations-reflexivity-symmetry-transitivity[405]; the other three are worked above. The three properties are independent, and most of the eight combinations appear here. Relations with all three, like $6 \mid (m-n)$, are **equivalence relations** (equivalence-relations[406]). Relations like $x \mid y$ — reflexive and transitive, with no two different elements related both ways — are **partial orders** (partial-order-relations[407]). Those are the next two topics in the course.

Symmetric and transitive do not make reflexive

> **Claim.** If a relation ρ on a set A is both symmetric and transitive, then ρ is reflexive. — **False.**

Counterexample. $A = \{1,2\}$, $\rho = \{(1,1)\}$. Symmetric: the only pair is $(1,1)$, whose reverse is itself. Transitive: the only two-step path is $1 \to 1 \to 1$, whose short cut $(1,1)$ is present. Not reflexive: $2 \not\rho\, 2$.

The tempting "proof" goes: *let $x \in A$; take y with $x \rho y$; by symmetry $y \rho x$; by transitivity $x \rho x$.* Every step is valid except the second. **Nothing guarantees there is any y with $x \rho y$.** The element 2 in the counterexample is related to nothing, so there is nothing to start the argument from. Adding the missing hypothesis makes the claim true:

> If ρ is symmetric and transitive, **and for each $x \in A$ there is some $y \in A$ with** $x \rho y$, then ρ is reflexive.

[405] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf
[406] courses/math1061/equivalence-relations.pdf
[407] courses/math1061/partial-order-relations.pdf

The proof is the tempting argument above, now legitimate. The picture is the right-hand panel of 2026-09-17-relations-reflexivity-symmetry-transitivity[408].

See also

- relations-on-sets[409] — relations as sets of pairs, the notation, arrow diagrams
- equivalence-relations[410] · partial-order-relations[411] — the two kinds of relation built from these properties, the second with antisymmetry[412] in place of symmetry
- quantified-statements[413] · proof-techniques[414] — why a "for all" needs a general argument and its negation needs a witness
- conditional-statements[415] — vacuous truth, which is why sparse relations are often symmetric and transitive
- sets-and-set-notation[416] — the proper-subset relation, and why it has no loops
- 2026-09-17-relations-reflexivity-symmetry-transitivity[417] — Lecture 23
- practice-problems[418] — §30, with full worked solutions

Sets and Set Notation

The language the rest of mathematics is written in: what a set is, the difference between belonging to one and being contained in one, and the operations that build new sets from old. See proving-set-properties[419] for the proof methods that go with these definitions, and functions-on-general-sets[420] for what gets built on top of them.

Writing a set down

Two ways, both used constantly:

- **By listing the elements**, inside braces: $\{1, 2, 3\}$, $\{a\}$, $\{\emptyset, \{\emptyset\}\}$. An infinite list gets an ellipsis: $\{\dots, -2, -1, 0, 1, 2, \dots\}$.

[408] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf
[409] courses/math1061/relations-on-sets.pdf
[410] courses/math1061/equivalence-relations.pdf
[411] courses/math1061/partial-order-relations.pdf
[412] courses/math1061/antisymmetric-relations.pdf
[413] courses/math1061/quantified-statements.pdf
[414] courses/math1061/proof-techniques.pdf
[415] courses/math1061/conditional-statements.pdf
[416] courses/math1061/sets-and-set-notation.pdf
[417] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf
[418] courses/math1061/practice-problems.pdf
[419] courses/math1061/proving-set-properties.pdf
[420] courses/math1061/functions-on-general-sets.pdf

- **By a defining condition** — *set-builder* notation: $\{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$, read "the set of integers n such that $n \equiv 2 \bmod 8$".

Both a vertical bar and a colon are used as the "such that" separator, interchangeably. $\{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$ and $\{(x, y) \mid x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$ take the bar; $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = 2x + 1\}$ and $f^{-1}(B) = \{x \in X : f(x) \in B\}$ take the colon. Read either as "such that"; nothing turns on which one is written.

Two conventions worth naming, because everything below relies on them: **sets take capital italic letters** (A, B, C, S, T, X, Y), with U reserved for the universal set, and **elements take lower case** (x, y, t, n). And $|A|$ denotes the **cardinality** of A — the number of elements it has (for infinite sets, where "number of elements" needs care, see cardinality[421]).

"Is an element of" versus "is a subset of"

> **Warning.** Take care with the distinction between *is an element of* ($\in$) and *is a subset of* ($\subseteq$).

This is the single most common source of error in the whole topic, and it is worth being blunt about why: the two relate **different kinds of thing**.

	Reads	Left-hand side is	Right-hand side is
$x \in A$	x is an element of A	an **object**	a **set**
$A \subseteq B$	A is a subset of B	a **set**	a **set**

Is $\mathbb{Z} \in \mathbb{Q}$? False. The elements of $\mathbb{Q}$ are rational *numbers*, and $\mathbb{Z}$ is not a number — it is a set of numbers. The true statement in the neighbourhood is $\mathbb{Z} \subseteq \mathbb{Q}$.

The instinct behind the mistake ("but aren't all integers rational?") is right; it is the symbol that is wrong. "All integers are rational" is exactly the claim $\mathbb{Z} \subseteq \mathbb{Q}$.

The same care applies one level down: **a single element is not the same as the set containing that element**, so $2 \neq \{2\}$.

Worked: true or false?

	Statement		Why
a)	$4 \in \{4\}$	**True**	$\{4\}$ contains 4 as an element

[421] courses/math1061/cardinality.pdf

	Statement		Why
b)	$4 \in \{\{4\}\}$	**False**	$\{\{4\}\}$ does not contain 4 as an element — it contains $\{4\}$ as an element
c)	$\{4\} \in \{2, 3, 4\}$	**False**	$\{2, 3, 4\}$ does not contain $\{4\}$ as an element — it contains 4 as an element

Each false line becomes true if you swap the symbol or the braces, which is the point of the exercise. In (c), $\{4\} \subseteq \{2, 3, 4\}$ **is** true.

The reliable technique: **write out the set's elements and ask whether the left-hand object is literally one of the things in the list.** For $\{\{4\}\}$ that list is a single item, the set $\{4\}$ — and 4 is not on it.

Subsets and proper subsets

> A set S is a **subset** of a set T, written $S \subseteq T$, if every element in S is also in T. Formally, $\forall x$, if $x \in S$ then $x \in T$.
>
> A set S is a **proper subset** of T, written $S \subset T$, if $S \subseteq T$ **and** there is an element in T that is not in S.

So $\subset$ is $\subseteq$ plus "and they are not equal" — exactly parallel to $<$ against $\leq$ for numbers.

	Holds	Fails
$\subseteq$	$\mathbb{Z} \subseteq \mathbb{Q}$, and $\mathbb{Z} \subseteq \mathbb{Z}$	
$\subset$	$\mathbb{Z} \subset \mathbb{Q}$	$\mathbb{Z} \not\subset \mathbb{Z}$

A set is always a subset of itself and never a *proper* subset of itself — that single line is the whole difference between the two symbols.

Proving one set is a subset of another

> To prove $S \subseteq T$, consider an **arbitrary** element of S and show it is also in T. That is: **suppose $x \in S$, and prove $x \in T$.**

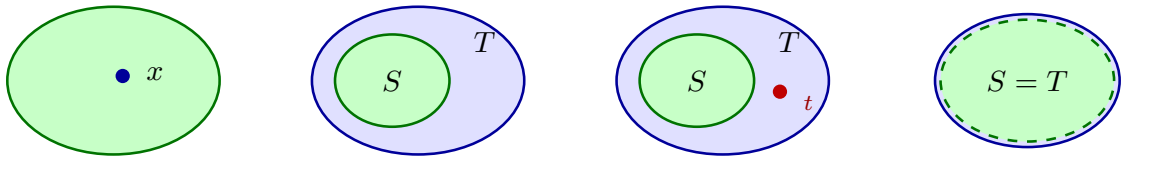


Figure 48: The four situations the symbols distinguish. An element sits inside a set; a subset is a set inside a set; a proper subset leaves something over; and equality is containment holding both ways at once. The contained set is green and the containing set pale blue, with elements as small blue dots; the red dot is the element that keeps the containment proper.

This is the *element method*, and it is used so heavily that proving-set-properties[422] treats it in full. The word doing the work is "arbitrary" — you may assume nothing about x beyond membership of S, which is what makes the one argument cover every element at once.

Worked. Let $D = \{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$ and let E be the set of even integers, i.e. $E = \{n \in \mathbb{Z} \mid n \equiv 0 \pmod 2\}$. Prove $D \subseteq E$.

Proof. Let $x \in D$. Then $x \equiv 2 \pmod 8$, so there exists $k \in \mathbb{Z}$ such that

$$x = 8k + 2 = 2(4k + 1) + 0$$

Since $4k + 1 \in \mathbb{Z}$, we have $x \equiv 0 \pmod 2$, and therefore $x \in E$. Thus $D \subseteq E$. ■

Rewriting $8k + 2$ as $2(4k + 1)$ is the entire proof — see modular-arithmetic[423] for the definition being applied.

Is $D \subset E$? Yes. We have $D \subseteq E$, and $4 \in E$ while $4 \notin D$ (since $4 \not\equiv 2 \bmod 8$), so the containment is proper. Note that upgrading $\subseteq$ to $\subset$ needs **one** witness, not a general argument.

When are two sets equal?

For sets S and T, $S = T$ means $\forall x$, $x \in S$ **if and only if** $x \in T$.

[422] courses/math1061/proving-set-properties.pdf
[423] courses/math1061/modular-arithmetic.pdf

Recall that $S \subseteq T$ means $\forall x$, if $x \in S$ then $x \in T$. Since $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$, it follows that

$$S = T \quad \text{is logically equivalent to} \quad (S \subseteq T) \wedge (T \subseteq S)$$

So **to prove two sets are equal, do two separate proofs**:

- Suppose $x \in S$, and prove $x \in T$. This shows $S \subseteq T$.
- Suppose $x \in T$, and prove $x \in S$. This shows $T \subseteq S$.

Together these give $S = T$. This is not a convention but a consequence — the double containment argument is just the biconditional law of logical-equivalence-laws[424] read through the definition of $\subseteq$, which is why "prove both directions" is never optional.

The empty set

$\emptyset = \{\ \}$ — the set with no elements.

Why is $\emptyset \subseteq A$ for every set A? Because "$\forall x$, if $x \in \emptyset$ then $x \in A$" is true for every set A. The hypothesis $x \in \emptyset$ is never satisfied, and a conditional with a false hypothesis is true — so the statement holds **vacuously**. See conditional-statements[425] for that truth-table row, which is doing all the work here.

Do not confuse this with $\emptyset \in A$. Some sets do contain the empty set as an element; many do not. $\emptyset \subseteq A$ is a theorem about every set; $\emptyset \in A$ is a claim about one particular set that usually fails.

Why is $A \subseteq A$ for every set A? Because "$\forall x$, if $x \in A$ then $x \in A$" is true for every set A — this one for the opposite reason, that the conclusion simply restates the hypothesis.

There is only one empty set

Lemma. There is only one empty set.

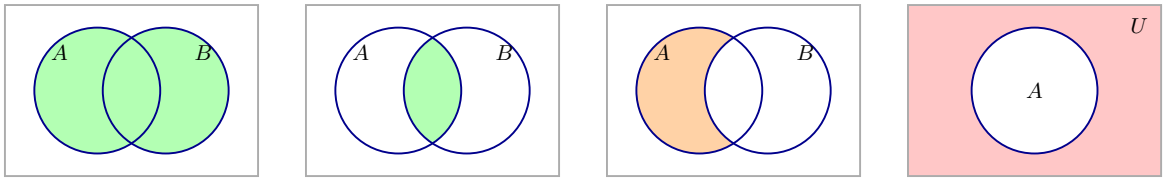
Proof (by contradiction). Suppose $\emptyset_1$ and $\emptyset_2$ are distinct sets each having no elements, so $\emptyset_1 \neq \emptyset_2$. Since $\emptyset_1$ has no elements, it is a subset of $\emptyset_2$; that is, $\emptyset_1 \subseteq \emptyset_2$. Also, since $\emptyset_2$ has no elements, $\emptyset_2 \subseteq \emptyset_1$. Thus $\emptyset_1 = \emptyset_2$ by definition of set equality — contradicting the supposition. ■

This is why we say *the* empty set and write a single symbol for it. The proof is a neat demonstration of the double-containment criterion doing real work: both containments come free from vacuous truth, and equality falls out.

[424] courses/math1061/logical-equivalence-laws.pdf
[425] courses/math1061/conditional-statements.pdf

Unions and intersections

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\} \qquad A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$



$A \cup B$ $A \cap B$ $A - B$ (also written $A \setminus B$) $A^c = U - A$

Figure 49: The four operations as shaded regions. Union takes everything in either circle, intersection only the overlap, difference removes B from A, and the complement is everything in the universe outside A — which is why a complement is only meaningful once the universe U is fixed. The enclosing rectangle is that universe.

Worked. Let $A_1 = \{1, 2, 3\}$, $A_2 = \{1, 2, 4\}$ and $A_3 = \{3, 4, 5\}$.

$$A_1 \cup A_2 = \{1, 2, 3, 4\} \qquad A_1 \cap A_2 = \{1, 2\} \qquad A_1 \cap A_3 = \{3\} \qquad A_2 \cap A_3 = \{4\}$$

Indexed over all three:

$$\bigcup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3 = \{1, 2, 3, 4, 5\} \qquad \bigcap_{i=1}^{3} A_i = (A_1 \cap A_2) \cap A_3 = \{1, 2\} \cap \{3, 4, 5\} = \emptyset$$

Worth noticing: **the three sets intersect pairwise in a non-empty set every time, and yet the triple intersection is empty.** Pairwise overlap does not survive to the whole family, so an indexed intersection has to be computed, not inferred.

Indexed families

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for } \textbf{at least one } i \in I\} \qquad \bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for } \textbf{every } i \in I\}$$

These extend to infinite index sets unchanged, which is where they earn their keep.

Worked, over $i = 0, 1, 2, \ldots$:

$$\bigcup_{i=0}^{\infty}\{i,-i\} = \{0\}\cup\{1,-1\}\cup\{2,-2\}\cup\cdots = \{\dots,-2,-1,0,1,2,\dots\} = \mathbb{Z}$$

$$\bigcap_{i=0}^{\infty}[-i,\,i] = \{0\}$$

recalling the interval notation $[a,b] = \{x \in \mathbb{R} \mid a \le x \le b\}$.

The intersection is the interesting one. The intervals **grow** as i increases, so the intersection is pinned by the *smallest* of them, the $i = 0$ term $[0,0] = \{0\}$. Every larger interval contains 0, so nothing is lost, and nothing else survives.

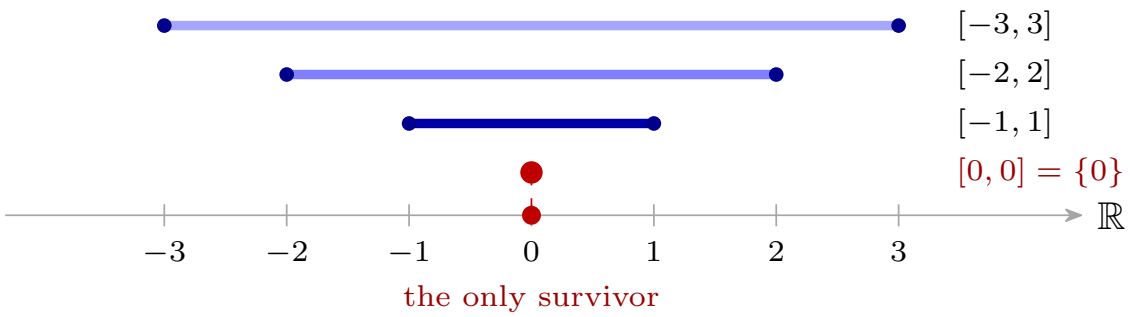


Figure 50: An intersection over an increasing family is decided by its smallest member. Each interval contains the one below it, so the only real number lying in all of them is the single point the innermost interval contains. The intervals sit above the number line, with a filled dot at each closed endpoint.

Set difference and complement

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

Both are drawn in Figure 49 above.

The backslash and the minus sign mean the same thing: $A - B$ can equally be written $A \setminus B$. Different textbooks pick different ones; there is no distinction to learn.

The **complement** A^c is the set difference from the universal set U under discussion: $A^c = U - A$. It is only meaningful once U is fixed, so a complement always sits inside a stated universe.

The power set

$\mathcal{P}(A)$ is the set of **all subsets** of A.

Worked. Let $S = \{1, 2, 3\}$. Then

$$\mathcal{P}(S) = \{\, \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\} \,\}$$

Note that the elements of $\mathcal{P}(S)$ are **sets**, which resets the $\in$ / $\subseteq$ trap one level up:

Statement		Why
$\{1,2\} \in \mathcal{P}(S)$	**True**	$\{1,2\}$ is one of the eight things listed
$\{1,2\} \subseteq \mathcal{P}(S)$	**False**	that would need 1 and 2 themselves to be elements of $\mathcal{P}(S)$, i.e. to be subsets of S — and they are numbers, not sets
$\{\{1,2\}\} \subseteq \mathcal{P}(S)$	**True**	the one element it has, $\{1,2\}$, is in $\mathcal{P}(S)$

Also worth recording as a standing fact: since $\emptyset \subseteq A$ for every set A, it follows that $\emptyset \in \mathcal{P}(A)$ for every set A. Every power set is non-empty, including $\mathcal{P}(\emptyset)$.

Fact. If T is a **finite** set with n elements, then $|\mathcal{P}(T)| = 2^n$.

The finiteness matters — the count is meaningless otherwise. The 2^n comes from building a subset by making n independent in/out choices. Sorting the same subsets by size instead gives $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$ (binomial-coefficients[426]).

Worked: is $\{1, 3, -1\} \subset \mathcal{P}(\mathbb{Z})$?

False, and the reasoning is the $\in$/$\subseteq$ distinction again, run carefully:

- $1, 3, -1 \in \mathbb{Z}$, so $\{1, 3, -1\} \subseteq \mathbb{Z}$.
- Therefore $\{1, 3, -1\} \in \mathcal{P}(\mathbb{Z})$ — it is one of the subsets of $\mathbb{Z}$, hence an *element* of the power set.
- So $\{1, 3, -1\} \not\subset \mathcal{P}(\mathbb{Z})$: for that, its **elements** 1, 3 and -1 would have to be elements of $\mathcal{P}(\mathbb{Z})$, i.e. subsets of $\mathbb{Z}$ — and they are integers, not sets.

The statement is off by exactly one level, which is the characteristic failure mode with power sets.

[426] courses/math1061/binomial-coefficients.pdf

Worked: power sets of power sets

Building up from the empty set, with the 2^n fact as a running check:

	Value	$\lvert\cdot\rvert$ of the input	Check
$\mathcal{P}(\{a\})$	$\{\emptyset,\ \{a\}\}$	$\lvert\{a\}\rvert = 1$	$2^1 = 2$ ✓
$\mathcal{P}(\emptyset)$	$\{\emptyset\}$	$\lvert\emptyset\rvert = 0$	$2^0 = 1$ ✓
$\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$	$\{\emptyset,\ \{\emptyset\}\}$	$\lvert\{\emptyset\}\rvert = 1$	$2^1 = 2$ ✓
$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\{\emptyset,\{\emptyset\}\})$	$\{\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\emptyset,\{\emptyset\}\}\}$	$\lvert\{\emptyset,\{\emptyset\}\}\rvert = 2$	$2^2 = 4$ ✓

$\mathcal{P}(\emptyset) = \{\emptyset\}$ is the line to get right: the empty set has exactly one subset — itself — so its power set has **one** element and is **not** empty. Counting the elements at each stage and checking against 2^n is the cheapest way to catch a dropped or duplicated brace.

Cartesian products

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

the set of **ordered pairs** with first coordinate from A and second from B.

Worked. $A_1 = \{1, 2\}$, $A_2 = \{3, 4, 5\}$, $A_3 = \{6\}$.

$$A_1 \times A_2 = \{(1,3), (1,4), (1,5), (2,3), (2,4), (2,5)\}$$

$$A_1 \times A_2 \times A_3 = \{(1,3,6), (1,4,6), (1,5,6), (2,3,6), (2,4,6), (2,5,6)\}$$

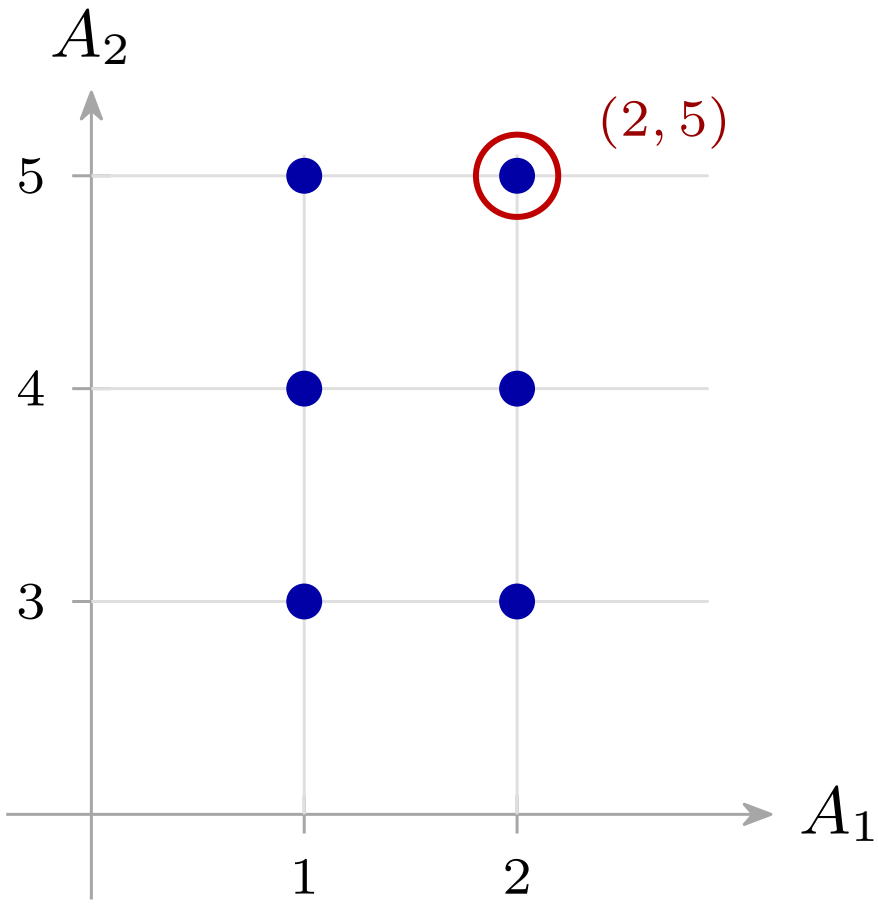
Worked. Let $S = \{a, b, c\}$ and $T = \{c, d\}$.

- $(d, c) \notin S \times T$, since $d \notin S$ — the **order matters**, and d is disqualified as a first coordinate.
- $(c, d) \in S \times T$, since $c \in S$ and $d \in T$.
- $S \times T$ contains $3 \times 2 = 6$ elements.

The familiar case is $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$, usually written $\mathbb{R}^2$ — the plane is a Cartesian product, which is where the name comes from.

Two facts:

- If $A = \emptyset$ or $B = \emptyset$ then $A \times B = \emptyset$ — there is no way to choose a coordinate from an empty set.
- For finite sets, $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.



$$|A_1 \times A_2| = |A_1| \cdot |A_2| = 2 \times 3 = 6$$

Figure 51: A Cartesian product laid out as a grid: one row per element of the first set, one column per element of the second, one ordered pair at every crossing. The rectangular shape is the counting fact — the number of pairs is the product of the two sizes.

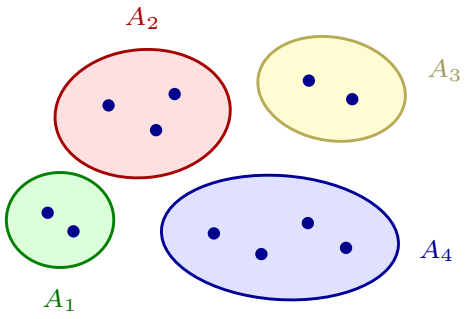
Notation clash to be aware of. (a, b) can mean an **ordered pair**, and (a, b) can also mean an **open interval** — the real numbers x with $a < x < b$. Nothing in the symbols distinguishes them; only the context does.

Partitions

A finite or infinite collection of **non-empty** sets $\{A_1, A_2, A_3, \dots\}$ is a **partition** of a set A if and only if

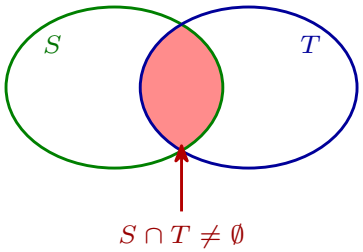
$$A = A_1 \cup A_2 \cup A_3 \cup \cdots \qquad \text{and} \qquad A_i \cap A_j = \emptyset \text{ for each } i, j \geq 1,\ i \neq j$$

Three conditions, all of which are checkable and all of which get tested: the pieces are **non-empty**, they **cover** A, and they are **pairwise disjoint**.



a partition of A

$A = A_1 \cup A_2 \cup A_3 \cup A_4$, pairwise disjoint



not a partition of R

$R = S \cup T$, but the pieces overlap

Figure 52: A partition cuts a set into non-empty pieces that cover it with no overlap — every element lands in exactly one piece. Failing any one of the three conditions is enough to disqualify a collection. On the left is a partition: separate closed curves, one per piece, each holding its elements as dots. On the right, two pieces share an element, so the collection is not a partition.

Examples over $\mathbb{Z}$:

- $\{E, O\}$, where E is the even integers and O the odd integers, is a partition of $\mathbb{Z}$.
- $\{\{0\},\ \mathbb{Z}^+,\ \mathbb{Z}^-\}$ is another partition of $\mathbb{Z}$ — a set can be partitioned in many ways.

Worked: a collection that fails

Let $S = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\}$, let $T = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 4\}$, and let $R = S \cup T$. **Is $\{S, T\}$ a partition of R?**

No. The covering condition holds by construction — $R = S \cup T$ is how R was defined. But disjointness fails:

$$10 = 3(3) + 1 \;\Rightarrow\; 10 \equiv 1 \pmod 3 \;\Rightarrow\; 10 \in S$$
$$10 = 4(2) + 2 \;\Rightarrow\; 10 \equiv 2 \pmod 4 \;\Rightarrow\; 10 \in T$$

so $10 \in S \cap T$ and $S \cap T \neq \emptyset$. Therefore $\{S, T\}$ is **not** a partition of R.

A single witness settles it — disjointness is a universal claim, so one counterexample is a complete disproof.

Worked: two partitions of $\mathbb{Z} \times \mathbb{Z}$

Any rule that sorts every pair into exactly one bucket works. Two independent ways:

By the sign of the first coordinate.

$$P = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \geq 0\} \qquad N = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a < 0\}$$

$\{N, P\}$ is a partition of $\mathbb{Z} \times \mathbb{Z}$ — every integer a is either ≥ 0 or < 0, never both.

By the parity of the second coordinate.

$$E = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \equiv 0 \pmod 2\} \qquad O = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \equiv 1 \pmod 2\}$$

$\{E, O\}$ is another partition of $\mathbb{Z} \times \mathbb{Z}$.

The recipe generalises: **take any property that every element either has or lacks, and the two resulting sets partition the whole** — provided neither comes out empty. That connection is made exact by equivalence relations: every partition is the set of classes of one, and the other way round (equivalence-classes-and-partitions[427]).

See also

- proving-set-properties[428] — the element method, the set identities, and proofs about these operations
- functions-on-general-sets[429] — functions defined as subsets of a Cartesian product
- equivalence-classes-and-partitions[430] — partitions as the classes of an equivalence relation
- modular-arithmetic[431] — the congruence sets used throughout the worked examples
- counting-principles[432] · counting-selections[433] — $|A \times B| = |A| \times |B|$ as the multiplication

[427] courses/math1061/equivalence-classes-and-partitions.pdf
[428] courses/math1061/proving-set-properties.pdf
[429] courses/math1061/functions-on-general-sets.pdf
[430] courses/math1061/equivalence-classes-and-partitions.pdf
[431] courses/math1061/modular-arithmetic.pdf
[432] courses/math1061/counting-principles.pdf
[433] courses/math1061/counting-selections.pdf

rule, and $\binom{n}{r}$, the number of r-element subsets of an n-element set
- inclusion-exclusion[434] · probability[435] — the size of a union of sets that overlap, with De Morgan's law for "neither", and events as subsets of a sample space
- pigeonhole-principle[436] — a partition as the set of pigeonholes
- conditional-statements[437] · logical-equivalence-laws[438] — vacuous truth, and the biconditional behind set equality
- 2026-09-03-set-theory-definitions[439] — Lecture 17
- practice-problems[440] — §21 Set Theory Definitions, with full worked solutions
- practice-problems[441] — §22 More Definitions and Examples of Sets

The Symmetric Group

S_n is the group whose elements are the bijections from $\{1, 2, \dots, n\}$ to itself, and whose operation is composition. Its elements are functions, not numbers, and it is the course's first group in which the order of a product matters. The definition of a group is in [groups], and the two ingredients are one-to-one-and-onto-functions[442] and composition-of-functions[443]. First met in 2026-09-24-definitions-and-examples-of-groups[444].

The definition

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

An element of S_n is a way of sending each of $1, \dots, n$ to one of $1, \dots, n$, so that no two go to the same place and every place is used. To combine two elements, do one and then the other.

How many elements. A bijection in S_3 can send 1 to any of three places. That leaves two places for 2, and then one for 3, so S_3 has $3 \cdot 2 \cdot 1 = 6$ elements. In general S_n has $n!$ elements, one for each arrangement of $1, \dots, n$ (counting-principles[445]).

[434] courses/math1061/inclusion-exclusion.pdf
[435] courses/math1061/probability.pdf
[436] courses/math1061/pigeonhole-principle.pdf
[437] courses/math1061/conditional-statements.pdf
[438] courses/math1061/logical-equivalence-laws.pdf
[439] courses/math1061/2026-09-03-set-theory-definitions.pdf
[440] courses/math1061/practice-problems.pdf
[441] courses/math1061/practice-problems.pdf
[442] courses/math1061/one-to-one-and-onto-functions.pdf
[443] courses/math1061/composition-of-functions.pdf
[444] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[445] courses/math1061/counting-principles.pdf

The six elements of S_3

They are named f_1 to f_6 here, and each can be drawn as an arrow diagram (2026-09-24-definitions-and-examples-of-groups[446]). Each can also be written as a set of pairs or as a list of values.

	As a set of pairs	$1 \mapsto$	$2 \mapsto$	$3 \mapsto$	What it does
f_1	$\{(1,1),(2,2),(3,3)\}$	1	2	3	nothing
f_2	$\{(1,2),(2,1),(3,3)\}$	2	1	3	swaps 1 and 2
f_3	$\{(1,3),(2,2),(3,1)\}$	3	2	1	swaps 1 and 3
f_4	$\{(1,1),(2,3),(3,2)\}$	1	3	2	swaps 2 and 3
f_5	$\{(1,2),(2,3),(3,1)\}$	2	3	1	moves all three
f_6	$\{(1,3),(2,1),(3,2)\}$	3	1	2	moves all three, the other way

The pair form is the definition of a function as a set of pairs (functions-on-general-sets[447]). The names $f_1, \ldots, f_6$ are just labels, and other sources number the six differently.

Composing

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

The function on the right acts first. To work out $f \circ g$, take each of 1, 2, 3 in turn, apply g, then apply f to the result.

$f_2 \circ f_3$: f_3 first, then f_2.

x	$f_3(x)$	$f_2(f_3(x))$
1	3	3
2	2	1
3	1	2

[446] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[447] courses/math1061/functions-on-general-sets.pdf

So $f_2 \circ f_3$ sends $1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 2$, which is f_6.

$f_3 \circ f_2$: f_2 first, then f_3.

x	$f_2(x)$	$f_3(f_2(x))$
1	2	2
2	1	3
3	3	1

So $f_3 \circ f_2$ sends $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, which is f_5.

The same two functions in the two orders give different answers. $f_2 \circ f_3 = f_6$ but $f_3 \circ f_2 = f_5$.

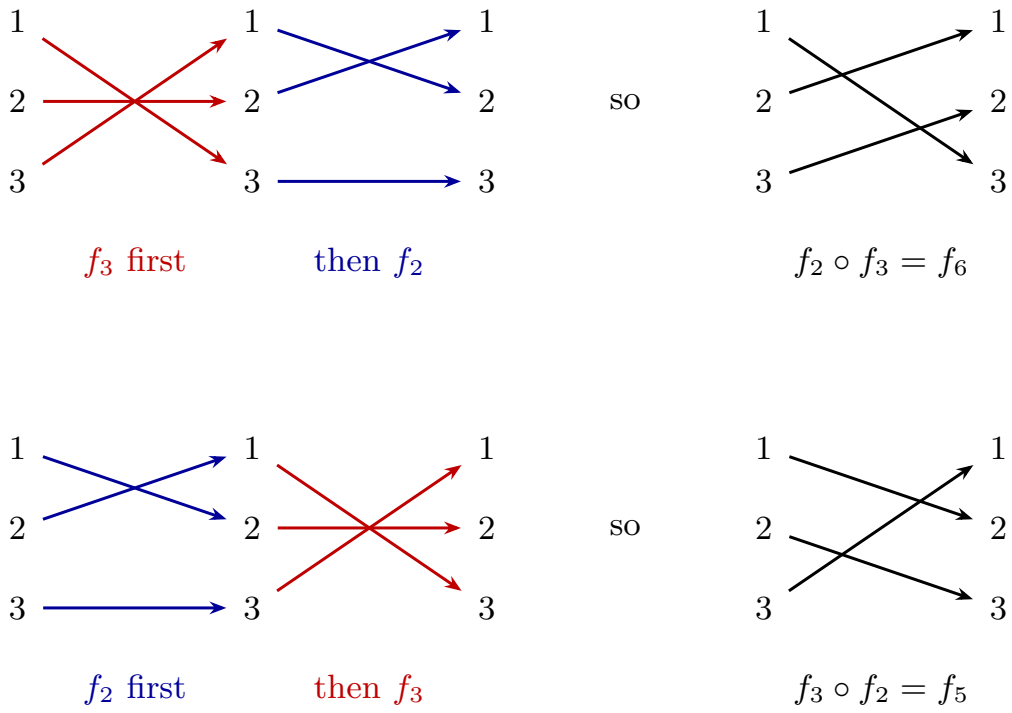


Figure 53: The same two elements of S_3 composed in both orders. Top: f_3 first and then f_2, which is $f_2 \circ f_3$. Following each number through both steps gives $1 \to 3$, $2 \to 1$, $3 \to 2$, the element f_6. Bottom: f_2 first and then f_3, which is $f_3 \circ f_2$. Now the result is $1 \to 2$, $2 \to 3$, $3 \to 1$, the element f_5. In each row the picture runs left to right in the order things happen, and the formula names the functions right to left.

Why it is a group

For S_3 the properties can be checked from its table, with associativity by a general argument (2026-09-24-definitions-and-examples-of-groups[448]). Each one also follows, for every n, from facts about functions:

- **Closure.** The composition of two bijections is a bijection (composition-of-functions[449]).
- **Associativity.** For any three functions, $f \circ (g \circ h)$ and $(f \circ g) \circ h$ both send x to $f(g(h(x)))$.
- **Identity.** The function that sends every number to itself, f_1 in S_3. Composing with it on either side changes nothing.
- **Inverses.** A bijection has an inverse function (inverse-functions[450]), which is again a bijection, and composing the two in either order gives the identity (composition-of-functions[451]).

So the inverse of f in the group S_n is the inverse function f^{-1}, and the two uses of the notation agree. In an arrow diagram the inverse is found by **reversing every arrow**.

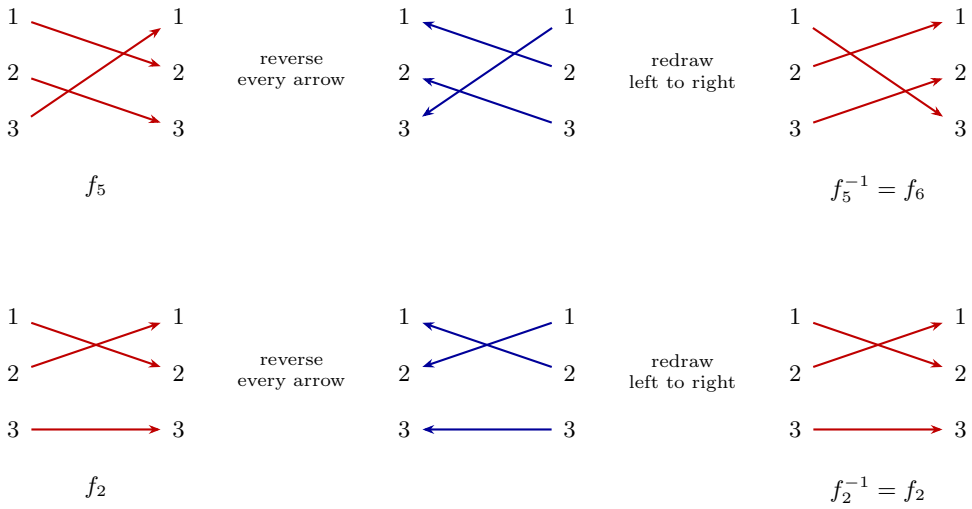


Figure 54: Inverses in S_3 by reversing arrows. Top: f_5 sends $1 \to 2$, $2 \to 3$, $3 \to 1$. Turning each arrow round gives $2 \to 1$, $3 \to 2$, $1 \to 3$, and reading that as a function of 1, 2, 3 gives $1 \to 3$, $2 \to 1$, $3 \to 2$, which is f_6. So $f_5^{-1} = f_6$. Bottom: f_2 swaps 1 and 2. Turning its arrows round gives the same diagram, so f_2 is its own inverse. The same holds for f_3 and f_4, the other two swaps.

[448] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[449] courses/math1061/composition-of-functions.pdf
[450] courses/math1061/inverse-functions.pdf
[451] courses/math1061/composition-of-functions.pdf

The Cayley table of S_3

The entry in the row of f and the column of g is $f \circ g$ (cayley-tables[452]).

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
$\mathbf{f_1}$	f_1	f_2	f_3	f_4	f_5	f_6
$\mathbf{f_2}$	f_2	f_1	f_6	f_5	f_4	f_3
$\mathbf{f_3}$	f_3	f_5	f_1	f_6	f_2	f_4
$\mathbf{f_4}$	f_4	f_6	f_5	f_1	f_3	f_2
$\mathbf{f_5}$	f_5	f_3	f_4	f_2	f_6	f_1
$\mathbf{f_6}$	f_6	f_4	f_2	f_3	f_1	f_5

Read off it:

- **Identity:** f_1.
- **Inverses:** $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_4$, $f_5^{-1} = f_6$, $f_6^{-1} = f_5$.
- **Not abelian:** $f_2 \circ f_3 = f_6$ but $f_3 \circ f_2 = f_5$.

The three swaps are their own inverses: doing a swap twice puts everything back. f_5 and f_6 undo each other. The table also shows $f_5 \circ f_5 = f_6$ and $f_6 \circ f_5 = f_1$, so doing f_5 three times returns everything to where it started.

Non-abelian does not mean nothing commutes. $f_5 \circ f_6 = f_6 \circ f_5 = f_1$, and f_1 commutes with everything. A group is non-abelian as soon as **one** pair fails to commute.

Powers and cyclic subgroups of S_3

Powers are defined in any group (subgroups-and-cyclic-groups[453]). In S_3 a power is a repeated composition, $f^2 = f \circ f$, and $f^0 = f_1$. Read from the table:

- f_5**.** $f_5^1 = f_5$, $f_5^2 = f_5 \circ f_5 = f_6$, $f_5^3 = f_5^2 \circ f_5 = f_6 \circ f_5 = f_1$. This is "doing f_5 three times returns everything to where it started": f_5 moves $1 \to 2 \to 3 \to 1$, and three moves bring each number home. So $\langle f_5 \rangle = \{f_5, f_6, f_1\}$.
- f_6**.** $f_6 = f_5^{-1}$, so $\langle f_6 \rangle = \langle f_5 \rangle$. Directly: $f_6^2 = f_6 \circ f_6 = f_5$ and $f_6^3 = f_5 \circ f_6 = f_1$.
- **The swaps.** $f_2^2 = f_2 \circ f_2 = f_1$, since swapping twice changes nothing. So $\langle f_2 \rangle = \{f_2, f_1\}$, and likewise $\langle f_3 \rangle = \{f_3, f_1\}$ and $\langle f_4 \rangle = \{f_4, f_1\}$.
- **The identity.** $\langle f_1 \rangle = \{f_1\}$.

[452] courses/math1061/cayley-tables.pdf
[453] courses/math1061/subgroups-and-cyclic-groups.pdf

a	Powers of a until f_1	$\langle a \rangle$
f_1	f_1	$\{f_1\}$
f_2	f_2, f_1	$\{f_1, f_2\}$
f_3	f_3, f_1	$\{f_1, f_3\}$
f_4	f_4, f_1	$\{f_1, f_4\}$
f_5	f_5, f_6, f_1	$\{f_1, f_5, f_6\}$
f_6	f_6, f_5, f_1	$\{f_1, f_5, f_6\}$

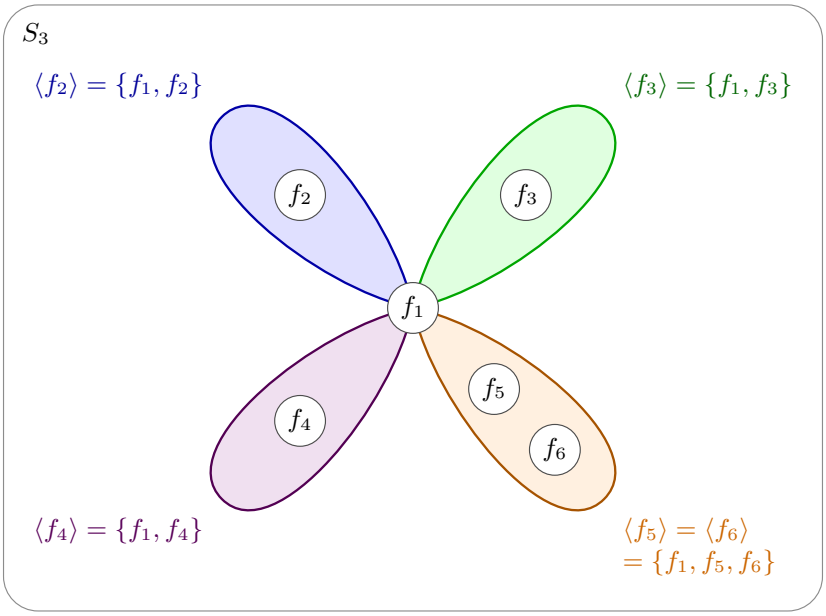


Figure 55: The cyclic subgroups of S_3, drawn inside it. Each petal is the set of powers of one element. The identity f_1, where the petals meet, is in every one, and it is the only element any two of them share. The three swaps f_2, f_3, f_4 each generate a subgroup of two elements, because a swap done twice changes nothing. f_5 and f_6 move all three numbers round and are each other's inverses, so they generate the same subgroup f_1, f_5, f_6. No petal is the whole of S_3, so no element generates it and S_3 is not cyclic.

None of the six is all of S_3, so S_3 **is not cyclic**. It could not have been: every cyclic group is abelian, and S_3 is not (subgroups-and-cyclic-groups[454]). $\{f_1, f_5, f_6\}$ also shows up as a block of the table when its elements are listed first (cayley-tables[455]).

[454] courses/math1061/subgroups-and-cyclic-groups.pdf
[455] courses/math1061/cayley-tables.pdf

Common mistakes

- **Composing in the wrong order.** $f \circ g$ means g first. Reading it left to right gives the other product, which in S_3 is usually a different element.
- **Reading the table as column $\circ$ row.**
- **Thinking S_3 has three elements.** It has six. The 3 is the size of the set being rearranged.
- **Treating the elements as numbers.** f_2 is a function. $f_2 \circ f_3$ is a composition, not a multiplication of 2 and 3.
- **Reading f^{-1} as $\frac{1}{f}$.** It is the inverse function.
- **Concluding from "non-abelian" that no two elements commute.**

See also

- [groups] — the definition, and abelian against non-abelian
- cayley-tables[456] — reading a table, and why its rows and columns have no repeats
- composition-of-functions[457] — the operation of S_n, and why it is done right to left
- one-to-one-and-onto-functions[458] · inverse-functions[459] — bijections and their inverses, the elements of S_n and their group inverses
- functions-on-general-sets[460] — a function as a set of pairs
- subgroups-and-cyclic-groups[461] — powers, cyclic subgroups, and why a non-abelian group cannot be cyclic
- 2026-09-24-definitions-and-examples-of-groups[462] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[463] — Lecture 27
- practice-problems[464] — §33, with full worked solutions

[456] courses/math1061/cayley-tables.pdf
[457] courses/math1061/composition-of-functions.pdf
[458] courses/math1061/one-to-one-and-onto-functions.pdf
[459] courses/math1061/inverse-functions.pdf
[460] courses/math1061/functions-on-general-sets.pdf
[461] courses/math1061/subgroups-and-cyclic-groups.pdf
[462] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[463] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[464] courses/math1061/practice-problems.pdf