MATH1061 — Week 10 Notes

Table of contents

Lecture 27 — Elementary Properties of Groups **1**
- Goals . . . 1
- A group inside a group . . . 2
- Worked: the functions $ax + b$ form a group . . . 3
- Subgroups . . . 5
- Worked: is $\mathbb{Z}$ a subgroup of $(\mathbb{R}, +)$? . . . 6
- Worked: is $\mathbb{R} - \{0\}$ a subgroup of $(\mathbb{R}, +)$? . . . 6
- Powers of an element . . . 6
- Worked: $[3]^4$ and $[3]^{-4}$ in $\mathbb{Z}_7 - \{[0]\}$ . . . 7
- Cyclic subgroups . . . 8
- Worked: $\langle 3 \rangle$ in $\mathbb{Z}_{11} - \{[0]\}$ . . . 8
- Worked: all the cyclic subgroups of $(\mathbb{Z}_8, +)$ . . . 10
- Cyclic groups . . . 11
- Worked: which of these groups are cyclic? . . . 11
- Worked: $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic . . . 12
- See also . . . 13

Lecture 28 — Definitions and Examples of Fields **14**
- Goals . . . 14
- Cyclic subgroups . . . 14
- Cyclic groups . . . 16
- The definition of a field . . . 18
- Fields already in use . . . 18
- Worked: is $(\mathbb{Z}_4, +, \cdot)$ a field? . . . 19
- Worked: which of these is a field? . . . 19
- Solving equations in a field . . . 20
- See also . . . 22

Reference material **23**
- Cayley Tables . . . 23

Composition of Functions 29
Fields 34
Groups 41
The Integers Modulo n 50
Inverse Functions 57
Practice Problems — the Semester-wide Set 61
Subgroups and Cyclic Groups 186
The Symmetric Group 196

Lecture 27 — Elementary Properties of Groups

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

Goals

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

A question to keep in mind:

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

A group inside a group

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

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

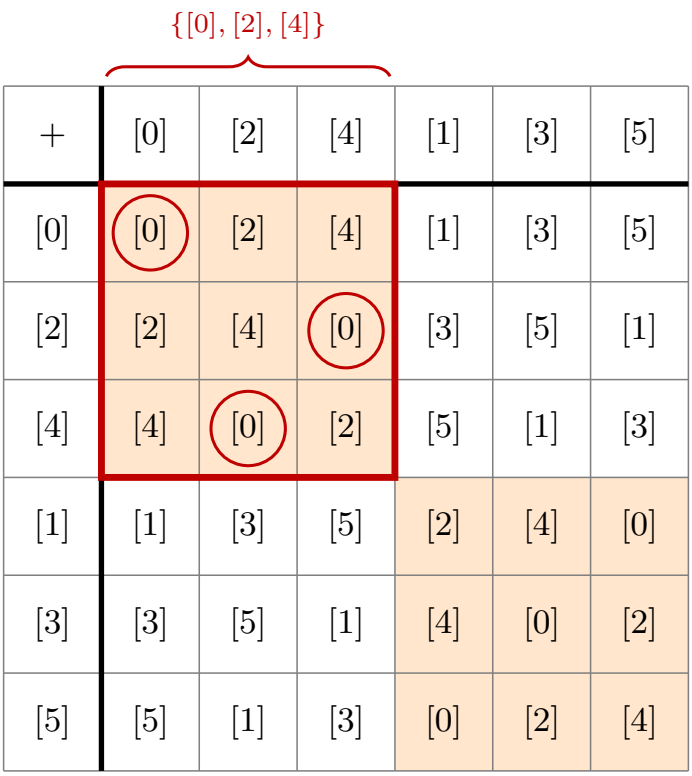


Figure 1: The table of $(\mathbb{Z}_6, +)$ with the even classes listed first. The top-left block, outlined, is a complete table on its own: its headings are $[0], [2], [4]$ and its body uses only $[0], [2], [4]$. So that set is closed under $+$, it contains the identity $[0]$, and the rings show each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

So $\{[0],[2],[4]\}$ is a group under the same operation as $\mathbb{Z}_6$, made of some of its elements. That is what a subgroup is. It is also exactly the set of multiples of $[2]$, $\{[2],[2]+[2],[2]+[2]+[2]\} = \{[2],[4],[0]\}$, which makes it the cyclic subgroup generated by $[2]$. Listing a subgroup's elements first, to make it a block, works for any subgroup of any finite group (cayley-tables[5]).

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

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

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

(1) Closure: for all $g, h \in G$, $g * h \in G$.

(2) Associativity: for all $g, h, k \in G$, $(g * h) * k = g * (h * k)$.

(3) Identity: $\exists e \in G$ such that $\forall g \in G$, $e * g = g * e = g$.

(4) Inverses: $\forall g \in G$, $\exists g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

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

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

Throughout, let

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

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

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

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

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

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

[5] courses/math1061/cayley-tables.pdf

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

and

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

The two agree for every x, so $(f\circ g)\circ h = f\circ(g\circ h)$. ✓ Composition of functions is always associative (groups[6]), so this could have been quoted; the algebra confirms it for this family.

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

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

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

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

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

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

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

[6] courses/math1061/groups.pdf

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

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

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

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

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

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

Two remarks:

- **Why $a \neq 0$.** With $a = 0$ the function $f(x) = b$ is constant. It sends everything to b, so nothing composed with it can give back x, and it has no inverse. Leaving out $a = 0$ is what makes F a group, in the same way that leaving out 0 turns $(\mathbb{R}, \cdot)$ into the group $(\mathbb{R} - \{0\}, \cdot)$.
- **F is not abelian.** In general $f \circ g = (ac)\,x + (ad + b)$ and $g \circ f = (ca)\,x + (cb + d)$ have different constants. With $f(x) = 2x$ and $g(x) = x + 1$, $(f \circ g)(x) = 2x + 2$ but $(g \circ f)(x) = 2x + 1$. So, like S_3 (symmetric-group[7]), this is a group in which the order of a composition matters.

Subgroups

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

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

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

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

Associativity is not on the list, because H inherits it. $(g*h)*k = g*(h*k)$ holds for all $g, h, k \in G$, so in particular it holds for all $g, h, k \in H$. G associative $\Rightarrow$ H associative under $*$. The other three can fail, because each one asks for an element to be *in* H. More on subgroups, and why the identity of H has to be the identity of G, is in subgroups-and-cyclic-groups[8].

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

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

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

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

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

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

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

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

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

The same set *is* a group under multiplication, $(\mathbb{R} - \{0\}, \cdot)$ (groups[9]). But a subgroup must use the operation of the group it sits in, and under $+$ it fails.

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

Powers of an element

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

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

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

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

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

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

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

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

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

and

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

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

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

The powers of a group element follow the same exponent rules as powers of a number. The laws for exponents of mixed sign, and a picture of the powers as a line or a loop, are in subgroups-and-cyclic-groups[10].

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

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

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

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

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

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

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

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

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

Check by the other route. $[3]^{-1} = [5]$, since $[3] \cdot [5] = [15] = [1]$. Then $[3]^{-4} = [5]^4 = [25] \cdot [25] = [4] \cdot [4] = [16] = [2]$. The same. And $[3]^4 \cdot [3]^{-4} = [4] \cdot [2] = [1] = [3]^0$, as the first law says it must be. Both inverses can also be read off the table of this group (2026-09-24-definitions-and-examples-of-groups[11]).

Cyclic subgroups

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

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

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

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

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

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

In a finite group, list the positive powers $a^1, a^2, a^3, \ldots$ until the list comes back to where it started. After that it only repeats, and the negative powers turn out to be in the list already (subgroups-and-cyclic-groups[12]).

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

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

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

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

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

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

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

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

$\langle 3 \rangle$ has 5 of the group's 10 elements, so 3 does not generate the whole group. Another element does: the powers of 2 are all ten elements (practice-problems[13], Q4).

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

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

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

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

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

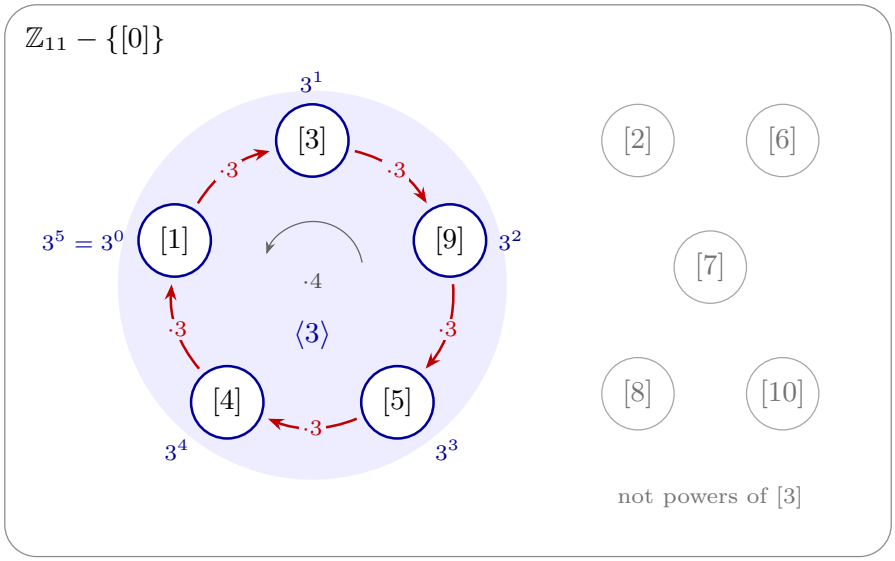


Figure 2: The powers of [3] in $\mathbb{Z}_{11} - [0]$. Each arrow multiplies by [3]. Starting from [3] the powers run $[3], [9], [5], [4], [1]$, and since $[3]^5 = [1]$ the next step is back at [3], so the powers go round a loop of five and $\langle 3 \rangle = 1, 3, 4, 5, 9$. Going round backwards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

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

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

Two rules were used:

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

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

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

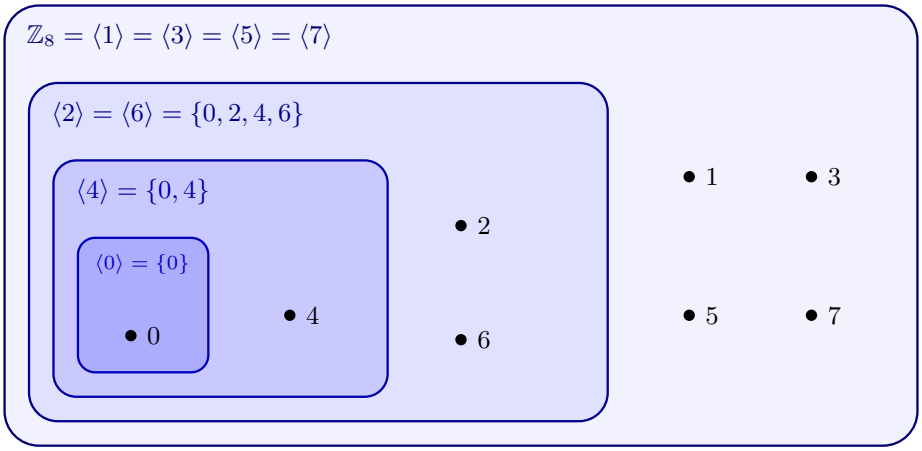


Figure 3: The four cyclic subgroups of $(\mathbb{Z}_8, +)$, each drawn inside the next. Every element generates exactly the smallest region it sits in: 0 generates only 0, 4 generates $0, 4$, 2 and 6 generate $0, 2, 4, 6$, and the four odd elements $1, 3, 5, 7$ each generate all of $\mathbb{Z}_8$. Elements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

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

Cyclic groups

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

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

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

How to prove a group is cyclic, and how to prove it is not, is in subgroups-and-cyclic-groups[14].

Worked: which of these groups are cyclic?

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

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

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

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

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

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

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

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

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

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

Either way $\langle a \rangle \neq \mathbb{Q}$, so $(\mathbb{Q}, +)$ is not cyclic. The multiples of any one rational are evenly spaced with gaps, and half of it falls in the first gap. A picture is in subgroups-and-cyclic-groups[15].

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

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

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

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

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

It works because the first coordinate comes back to 0 every 2 steps and the second every 3 steps, and the two are back at 0 together for the first time at step 6. Not every element generates: $(0, 1)$ gives only $\{(0,0), (0,1), (0,2)\}$ and $(1, 0)$ only $\{(0,0), (1,0)\}$. These three are drawn in subgroups-and-cyclic-groups[16].

See also

- subgroups-and-cyclic-groups[17] — subgroups, powers and the power laws, $\langle a \rangle$, and cyclic groups, with more examples
- [groups] — the four properties, and the elementary properties: unique identity and inverses, the inverse of a product
- cayley-tables[18] — reading a subgroup off a table by listing its elements first

[15] courses/math1061/subgroups-and-cyclic-groups.pdf
[16] courses/math1061/subgroups-and-cyclic-groups.pdf
[17] courses/math1061/subgroups-and-cyclic-groups.pdf
[18] courses/math1061/cayley-tables.pdf

- integers-modulo-n[19] — $\mathbb{Z}_n$ and $\mathbb{Z}_n - \{[0]\}$, the groups most of the examples live in
- composition-of-functions[20] · inverse-functions[21] — the operation and the inverses in the group $(F, \circ)$
- symmetric-group[22] — the cyclic subgroups of S_3, which is not cyclic
- 2026-09-24-definitions-and-examples-of-groups[23] — Lecture 26 · 2026-10-08-definitions-and-examples-of-fields[24] — Lecture 28
- practice-problems[25] — §34, with full worked solutions

Lecture 28 — Definitions and Examples of Fields

The cyclic subgroups of $\mathbb{Z}_8$ and which groups are cyclic, then fields: a set with two operations that is an abelian group under each of them, joined by the distributive laws. Which of $\mathbb{Z}$, $\mathbb{Z}_4$, $\mathbb{Z}_7$ and $\mathbb{Z}_{15}$ are fields, and how to solve a linear equation in $\mathbb{Z}_{11}$ and $\mathbb{Z}_{17}$. Pre-work: Video 036 (Definitions and Examples of Fields). Fields are collected in [fields], cyclic subgroups and cyclic groups in subgroups-and-cyclic-groups[26], and $\mathbb{Z}_p$ and multiplicative inverses mod p in integers-modulo-n[27]. The group definition everything here leans on is in [groups].

Goals

1. Review the concepts of **groups**, **abelian groups**, **subgroups** and **cyclic subgroups**.
2. Become familiar with calculations in **fields**.
3. Learn how to solve equations in fields.

The four terms in the first goal, in one line each:

- **Group.** A set with a binary operation, $(G, *)$, satisfying closure, associativity, identity and inverses (groups[28]).
- **Abelian.** $a * b = b * a$ for all $a, b \in G$.
- **Subgroup.** A subset of G that is a group under the same operation (subgroups-and-cyclic-groups[29]).
- **Cyclic subgroup.** $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$, every power of a: positive, zero and negative.

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

Cyclic subgroups

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

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

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

The powers are taken with the group's own operation: $a^2 = a * a$, $a^0 = e$, and $a^{-i} = (a^{-1})^i$. In an additive group such as $(\mathbb{Z}_n, +)$ a "power" is a repeated sum, so $[a]^i = [ia]$, and $\langle [a] \rangle$ is the set of multiples of $[a]$. The full treatment is in subgroups-and-cyclic-groups[30].

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

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

$\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$, so there are eight elements to try. For each, keep adding $[a]$ until the sum comes back to $[0]$; after that the list repeats. The negative powers add nothing new: if k copies of $[a]$ make $[0]$, then $[a]^{-1} = [a]^{k-1}$, so every negative power is already one of the positive ones.

$$\begin{aligned}
\langle [0] \rangle &= \{[0]\} \\
\langle [1] \rangle &= \{[1], [2], [3], [4], [5], [6], [7], [8] = [0]\} = \mathbb{Z}_8 \\
\langle [2] \rangle &= \{[2], [4], [6], [8] = [0]\} = \{[0], [2], [4], [6]\} \\
\langle [3] \rangle &= \{[3], [6], [9] = [1], [4], [7], [10] = [2], [5], [8] = [0]\} = \mathbb{Z}_8 \\
\langle [4] \rangle &= \{[4], [8] = [0]\} = \{[0], [4]\}
\end{aligned}$$

The other three, $\langle [5] \rangle$, $\langle [6] \rangle$ and $\langle [7] \rangle$, need no new work, because of two rules that hold in any group:

- $\langle e \rangle = \{e\}$**.** Every power of the identity is the identity. That is $\langle [0] \rangle = \{[0]\}$ above.
- $\langle a \rangle = \langle a^{-1} \rangle$**.** The powers of a^{-1} are $(a^{-1})^i = a^{-i}$, and as i runs through $\mathbb{Z}$ so does $-i$. The two lists are the same powers taken in the opposite order.

In $(\mathbb{Z}_8, +)$ the inverse of $[a]$ is $[-a] = [8 - a]$, so $[5] = [3]^{-1}$, $[6] = [2]^{-1}$ and $[7] = [1]^{-1}$:

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

So $\mathbb{Z}_8$ has four distinct cyclic subgroups, $\{[0]\}$, $\{[0], [4]\}$, $\{[0], [2], [4], [6]\}$ and $\mathbb{Z}_8$ itself, and

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

$$\langle [1] \rangle = \langle [3] \rangle = \langle [5] \rangle = \langle [7] \rangle = \mathbb{Z}_8.$$

The four elements that reach everything are the odd ones. An even step from [0] only ever lands on even classes. The four subgroups sit inside one another, $\{[0]\} \subseteq \{[0],[4]\} \subseteq \{[0],[2],[4],[6]\} \subseteq \mathbb{Z}_8$, as drawn in 2026-10-06-elementary-properties-of-groups[31].

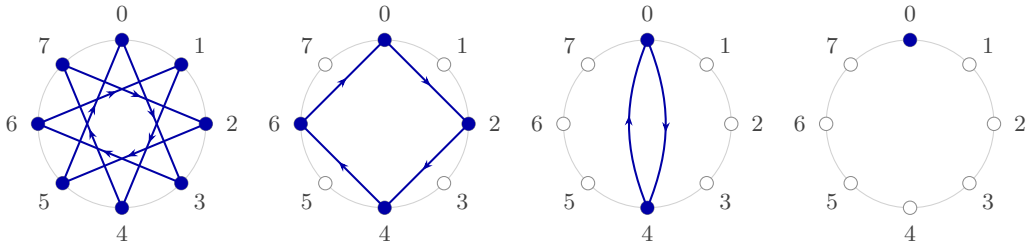


Figure 4: Each cyclic subgroup of $\mathbb{Z}_8$ as a walk round the eight classes, written without brackets, taking steps of a from 0 until the walk closes. Filled dots are the classes reached, and they make up $\langle a \rangle$. Steps of 3 visit all eight classes before returning, so $\langle 3 \rangle = \mathbb{Z}_8$. Steps of 2 visit only the even classes, steps of 4 only 0 and 4, and steps of 0 never leave 0. Steps of 5, 6 and 7 trace the same walks as steps of 3, 2 and 1, run backwards, which is why $\langle a \rangle = \langle a^{-1} \rangle$.

Cyclic groups

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

Such an a is a **generator** of G. Every element of a cyclic group is a power of the one element a. By the last section, $(\mathbb{Z}_8, +)$ is cyclic, with four generators. More on cyclic groups is in subgroups-and-cyclic-groups[32].

Worked: which of these groups are cyclic?

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

Group	Cyclic?	Generator
$(\mathbb{Z}_{10}, +)$	**yes**	[1]
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	**yes**	[2]

[31] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[32] courses/math1061/subgroups-and-cyclic-groups.pdf

Group	Cyclic?	Generator
$(\mathbb{Z}, +)$	**yes**	1
$(\mathbb{Q}, +)$	**no**	none

$(\mathbb{Z}_{10}, +)$**.** The multiples of $[1]$ are $[1], [2], \dots, [9], [10] = [0]$, all ten classes. So $\mathbb{Z}_{10} = \langle [1] \rangle$.

$(\mathbb{Z}_5 - \{[0]\}, \cdot)$**.** The set is $\{[1], [2], [3], [4]\}$ and the operation is multiplication, so here powers really are powers. $\langle [1] \rangle = \{[1]\}$, since $[1]$ is the identity. Trying $[2]$:

$$[2]^1 = [2], \quad [2]^2 = [4], \quad [2]^3 = [8] = [3], \quad [2]^4 = [16] = [1].$$

So $\langle [2] \rangle = \{[2], [4], [3], [1]\} = \mathbb{Z}_5 - \{[0]\}$, and the group is cyclic. A generator only has to exist; $[1]$ failing does not matter.

$(\mathbb{Z}, +)$**.** In additive notation 1^n is n copies of 1 added together, $1^0 = 0$, and $1^{-1} = -1$. So

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

An infinite group can be cyclic.

$(\mathbb{Q}, +)$**.** To show no generator exists, take an arbitrary rational r and find a rational that is not in $\langle r \rangle$. In $(\mathbb{Q}, +)$, $\langle r \rangle = \{kr : k \in \mathbb{Z}\}$, the integer multiples of r.

- *If* $r = 0$, then $\langle 0 \rangle = \{0\}$, which is not $\mathbb{Q}$.
- *If* $r \neq 0$, write $r = \frac{p}{q}$ with $p, q \in \mathbb{Z}$, $q \neq 0$. Then $\frac{p}{2q} = \frac{r}{2}$ is rational. If it were in $\langle r \rangle$ there would be a $k \in \mathbb{Z}$ with $\frac{r}{2} = kr$, and dividing by $r \neq 0$ gives $k = \frac{1}{2}$, which is not an integer. So $\frac{p}{2q} \notin \langle \frac{p}{q} \rangle$.

Either way $\langle r \rangle \neq \mathbb{Q}$, so $(\mathbb{Q}, +)$ is not cyclic. The case $r = 0$ has to be split off because $\frac{0}{2q} = 0$ *is* in $\langle 0 \rangle$. On the number line, $\langle r \rangle$ is a row of equally spaced points, and $\frac{r}{2}$ sits in the first gap (subgroups-and-cyclic-groups[33] draws it).

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

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

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

The elements are the six pairs (a, b) with $a \in \{0, 1\}$ and $b \in \{0, 1, 2\}$, and the operation adds each coordinate in its own modulus. Try $(a, b) = (1, 1)$, adding $(1, 1)$ each time:

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

The six powers are six different pairs, so they are all of $\mathbb{Z}_2 \times \mathbb{Z}_3$, and

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle. \qquad //$$

Not every element works. $(1, 0)$ only reaches $(1, 0)$ and $(0, 0)$, and $(0, 1)$ only reaches the three pairs with first coordinate 0. $(1, 1)$ works because its first coordinate cycles with period 2 and its second with period 3, and the two are not back at $(0, 0)$ together until the sixth step. The three cyclic subgroups are drawn side by side in subgroups-and-cyclic-groups[34].

The definition of a field

> **Definition.** A **field** $(F, +, \cdot)$ is a set F with two binary operations $+$ and $\cdot$ such that
>
> **(1)** $(F, +)$ is an abelian group;
>
> **(2)** $(F - \{0\}, \cdot)$ is an abelian group, where 0 is the identity of $(F, +)$; and
>
> **(3)** for all $f, g, h \in F$, $f \cdot (g + h) = (f \cdot g) + (f \cdot h)$ and $(f + g) \cdot h = (f \cdot h) + (g \cdot h)$.

Condition (3) is the pair of **distributive laws**. They are the only condition that involves both operations at once; without them $+$ and $\cdot$ would be two unrelated groups that happen to share a set.

Condition (1) is five checks: closure, associativity, identity and inverses for $+$, and commutativity to make it abelian. Condition (2) is the same five for $\cdot$, on the smaller set $F - \{0\}$. The "0" there means the additive identity, whatever it is called in F; in $\mathbb{Z}_n$ it is $[0]$. Why it has to be removed, and a picture of the two groups, are in fields[35].

[34] courses/math1061/subgroups-and-cyclic-groups.pdf
[35] courses/math1061/fields.pdf

Fields already in use

$(\mathbb{R}, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$ are fields. Arithmetic in them uses both kinds of inverse:

- **subtraction** is adding an additive inverse, $a - b = a + (-b)$;
- **division** is multiplying by a multiplicative inverse, $a \div b = a \cdot b^{-1}$ for $b \neq 0$.

Example. Solve $2x + 3 = 8$ in $\mathbb{R}$. Add -3 to both sides to get $2x = 5$, then multiply both sides by $2^{-1} = \frac{1}{2}$ to get $x = \frac{5}{2}$.

Those two steps are all that solving a linear equation needs, and the field axioms are what guarantee they can be done. The same two steps work in any field, including those where -3 and 2^{-1} are classes mod p.

Worked: is $(\mathbb{Z}_4, +, \cdot)$ a field?

Is $(\mathbb{Z}_4, +, \cdot)$ a field?

No. Condition (1) holds but condition (2) fails.

(1) $(\mathbb{Z}_4, +)$ is an abelian group with identity $[0]$. From the table: closure (only $[0], \ldots, [3]$ appear), associativity (inherited from addition of integers), identity $[0]$ (its row and column repeat the headings), inverses ($[0]$ is in every row: $-[1] = [3]$, $-[2] = [2]$, $-[3] = [1]$), and commutative (the table is symmetric about its diagonal).

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[\mathbf{0}]$	$[0]$	$[1]$	$[2]$	$[3]$
$[\mathbf{1}]$	$[1]$	$[2]$	$[3]$	$[0]$
$[\mathbf{2}]$	$[2]$	$[3]$	$[0]$	$[1]$
$[\mathbf{3}]$	$[3]$	$[0]$	$[1]$	$[2]$

(2) $(\mathbb{Z}_4 - \{[0]\}, \cdot)$ is not a group. The set is $\{[1], [2], [3]\}$:

$\cdot$	$[1]$	$[2]$	$[3]$
$[\mathbf{1}]$	$[1]$	$[2]$	$[3]$
$[\mathbf{2}]$	$[2]$	$[\mathbf{0}]$	$[2]$
$[\mathbf{3}]$	$[3]$	$[2]$	$[1]$

$[2] \cdot [2] = [4] = [0]$, and $[0] \notin \mathbb{Z}_4 - \{[0]\}$. **Closure fails.** Two non-zero classes multiply to zero. The same row shows a second failure: the row of $[2]$ has no $[1]$ in it, so $[2]$ has no multiplicative inverse either.

Worked: which of these is a field?

Two rules to use:

- $(\mathbb{Z}_n, +)$ **is a group for every** $n \in \mathbb{Z}^+$ (integers-modulo-n[36]). It is abelian, so condition (1) always holds for $\mathbb{Z}_n$.
- $(\mathbb{Z}_p, +, \cdot)$ **is a field when** p **is prime.** Why, and why a composite n never works, is in fields[37].

Which of the following is a field? (a) $(\mathbb{Z}, +, \cdot)$ (b) $(\mathbb{Z}_7, +, \cdot)$ (c) $(\mathbb{Z}_{15}, +, \cdot)$

(a) $(\mathbb{Z}, +, \cdot)$**: not a field.**

1. $(\mathbb{Z}, +)$ is an abelian group with identity 0. ✓
2. $(\mathbb{Z} - \{0\}, \cdot)$ is not a group, because 2 has no inverse: the identity is 1, and $2 \cdot y = 1$ needs $y = \frac{1}{2} \notin \mathbb{Z}$. ×

So $(\mathbb{Z}, +, \cdot)$ is not a field. This is where the second step of solving an equation breaks down in $\mathbb{Z}$: there is no 2^{-1} to multiply $2x = 5$ by, and indeed no integer x has $2x = 5$.

(b) $(\mathbb{Z}_7, +, \cdot)$**: a field,** since 7 is prime. Checking each condition directly:

1. $(\mathbb{Z}_7, +)$ is an abelian group with identity $[0]$, by the first rule. ✓
2. $(\mathbb{Z}_7 - \{[0]\}, \cdot)$ is the abelian group whose table is worked in 2026-09-24-definitions-and-examples-of-groups[38]. Its inverses are $[1]^{-1} = [1]$, $[2]^{-1} = [4]$, $[3]^{-1} = [5]$, $[6]^{-1} = [6]$. ✓
3. The distributive laws are inherited from the integers: $[a] \cdot ([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$, and the other law follows the same way. ✓

(c) $(\mathbb{Z}_{15}, +, \cdot)$**: not a field.**

1. $(\mathbb{Z}_{15}, +)$ is an abelian group with identity $[0]$. ✓
2. $(\mathbb{Z}_{15} - \{[0]\}, \cdot)$ is not a group: $[3] \cdot [5] = [15] = [0]$, which is not in the set, so closure fails. ×

So $(\mathbb{Z}_{15}, +, \cdot)$ is not a field. The factorisation $15 = 3 \cdot 5$ is exactly what produces the two non-zero classes with product $[0]$.

[36] courses/math1061/integers-modulo-n.pdf
[37] courses/math1061/fields.pdf
[38] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

Solving equations in a field

In a field, a linear equation is solved exactly as in $\mathbb{R}$: add the additive inverse of the constant to both sides, then multiply both sides by the multiplicative inverse of the coefficient. In $\mathbb{Z}_p$ both inverses are classes, and the multiplicative one has to be found. The general method, with a picture, is in fields[39].

Worked: linear equations in $\mathbb{Z}_{11}$ and $\mathbb{Z}_{17}$

(a) Solve the equation $2x + 3 = 8$ in the field $(\mathbb{Z}_{11}, +, \cdot)$. Hence determine the smallest positive integer y such that $2y + 3 \equiv 8 \pmod{11}$.

(b) Solve the equation $10x + 9 = 6$ in the field $(\mathbb{Z}_{17}, +, \cdot)$. Hence determine the smallest positive integer y such that $10y + 9 \equiv 6 \pmod{17}$.

(a) Work mod 11, writing 2 for [2] and so on inside the equation.

$$
\begin{aligned}
2x + 3 &= 8 && \\
2x + 3 + (-3) &= 8 + (-3) && \text{add the additive inverse of 3, } [-3] = [8] \\
2x &= 5 && \\
6 \cdot 2x &= 6 \cdot 5 && \text{multiply by the multiplicative inverse of 2, which is 6} \\
[12]x &= [30] && \\
1 \cdot x &= 8 && [12] = [1] \text{ and } [30] = [8] \\
x &= [8] &&
\end{aligned}
$$

The inverse of [2] is [6] because $2 \cdot 6 = 12 \equiv 1 \pmod{11}$.

Check: $2(8) + 3 = 19 \equiv 8 \pmod{11}$. ✓

The integers y with $2y + 3 \equiv 8 \pmod{11}$ are exactly the members of the solution class $[8] = \{\dots, -14, -3, 8, 19, 30, \dots\}$. The smallest positive one is $\mathbf{y = 8}$.

(b) Work mod 17.

$$
\begin{aligned}
10x + 9 &= 6 && \\
10x + 9 + (-9) &= 6 + (-9) && \text{add the additive inverse of 9, } [-9] = [8] \\
10x &= -3 && \\
12 \cdot 10x &= 12 \cdot (-3) && \text{multiply by the multiplicative inverse of 10, which is 12} \\
1 \cdot x &= -36 && [120] = [1] \\
x &= [-36] = [-2] = [15] && -36 = (-2) \cdot 17 - 2
\end{aligned}
$$

[39] courses/math1061/fields.pdf

Finding $[10]^{-1}$. In part (a) the inverse of $[2]$ could be seen at once from $2 \cdot 6 = 12$. Here it takes a search: list the multiples of 10 mod 17 until one is $\equiv 1$. Each line is the previous one plus 10, with 17 taken off whenever the total passes 16:

k	1	2	3	4	5	6	7	8	9	10	11	12
$10k \bmod 17$	10	3	13	6	16	9	2	12	5	15	8	**1**

$10 \cdot 12 = 120 = 7 \cdot 17 + 1$, so $[10]^{-1} = [12]$. Along the way, $10 \cdot 5 = 50 \equiv 16 = -1$, which is another route: $[10]^{-1} = -[5] = [12]$.

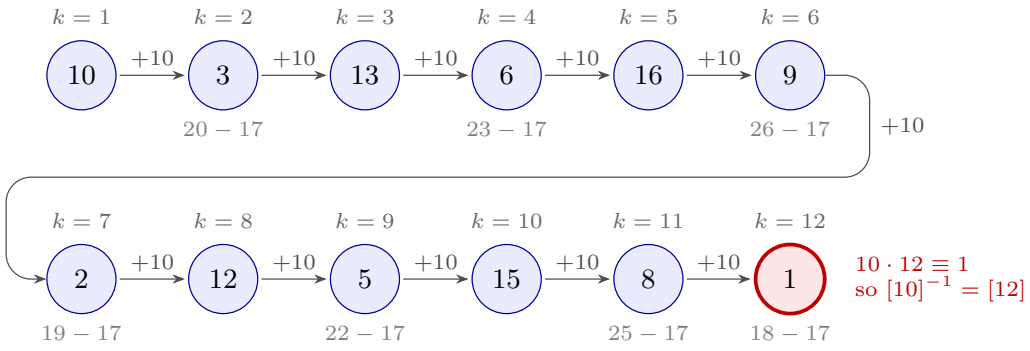


Figure 5: Searching for the inverse of $[10]$ in $\mathbb{Z}_{17}$. Starting at 10, each hop adds 10 and reduces mod 17; the grey number under a class is the unreduced total, shown where 17 had to be taken off. Because 17 is prime, the hops pass through non-zero classes only and cannot repeat before every non-zero class has appeared, so the class 1 is certain to turn up. It turns up at the twelfth multiple, so $10 \cdot 12 \equiv 1 \pmod{17}$ and $[10]^{-1} = [12]$.

Reducing the answer. $-36 = (-2) \cdot 17 - 2$, so $[-36] = [-2]$, and $[-2] = [-2 + 17] = [15]$. A shorter path is to notice $[12] = [-5]$, so $x = [-5] \cdot [-3] = [15]$ straight away.

Check: $10(15) + 9 = 159 = 10 \cdot 17 - 11 \equiv -11 \equiv 6 \pmod{17}$. ✓

The integers y with $10y + 9 \equiv 6 \pmod{17}$ are the members of $[15] = \{\dots, -19, -2, 15, 32, \dots\}$. The smallest positive one is $\mathbf{y = -2 + 17 = 15}$. The representative -2 is a correct name for the class, but it is not the positive integer the question asks for.

See also

- [fields] — the definition, examples and non-examples, why $\mathbb{Z}_n$ is a field exactly when n is prime, and solving equations

- subgroups-and-cyclic-groups[40] — subgroups, $\langle a \rangle$, and cyclic groups
- integers-modulo-n[41] — $\mathbb{Z}_n$, and multiplicative inverses mod p
- [groups] — the four group properties used in conditions (1) and (2)
- cayley-tables[42] — reading closure and inverses off a table, as in the $\mathbb{Z}_4$ question
- 2026-10-06-elementary-properties-of-groups[43] — Lecture 27 · 2026-10-12-introduction-to-counting[44] — Lecture 29
- practice-problems[45] — §34, where Q4 shows that $(\mathbb{Z}_{11} - \{[0]\}, \cdot)$ is cyclic
- practice-problems[46] — §36, with full worked solutions

Reference material

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[47]. With the right ordering of the headings, a subgroup shows up as a block of the table (below, and subgroups-and-cyclic-groups[48]).

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

Reading the properties off a table

[40] courses/math1061/subgroups-and-cyclic-groups.pdf
[41] courses/math1061/integers-modulo-n.pdf
[42] courses/math1061/cayley-tables.pdf
[43] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[44] courses/math1061/2026-10-12-introduction-to-counting.pdf
[45] courses/math1061/practice-problems.pdf
[46] courses/math1061/practice-problems.pdf
[47] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[48] courses/math1061/subgroups-and-cyclic-groups.pdf
[49] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

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[50]).

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[51], Q4.

Rows and columns have no repeats

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

Rows. By contradiction (2026-09-24-definitions-and-examples-of-groups[52]). Suppose row a has the same entry x in two different columns $b \neq c$, so $a * b = a * c$. Apply a^{-1} on the **left** of both sides:

[50] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[51] courses/math1061/practice-problems.pdf
[52] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf

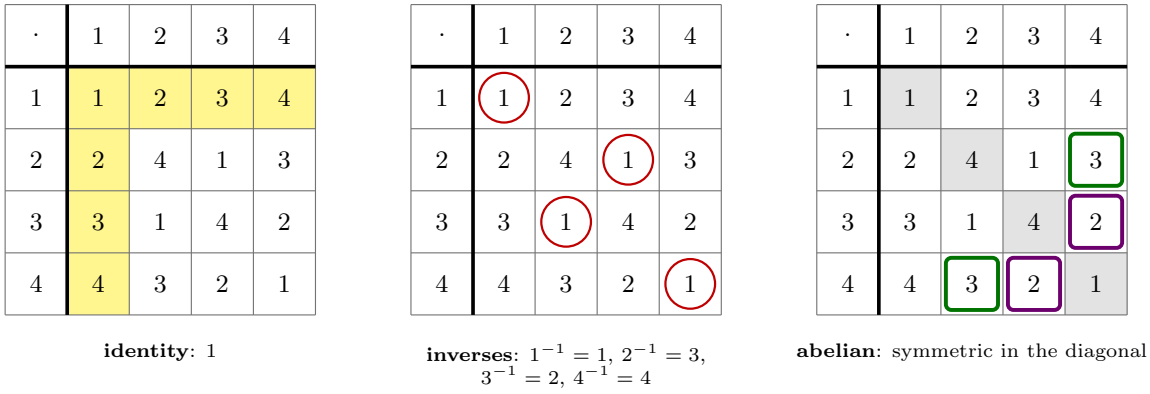


Figure 6: Three readings of one table, $\mathbb{Z}_5 - [0]$ under multiplication, written without brackets. Left: the row and the column of 1, in yellow, repeat the headings, so 1 is the identity. Middle: the identity appears once in every row. The ring in row 2 is in column 3, so $2^{-1} = 3$; the rings 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.

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

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

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

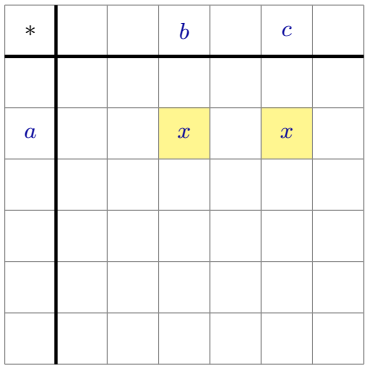
$$(b * a) * a^{-1} = (c * a) * a^{-1} \implies b * (a * a^{-1}) = c * (a * a^{-1}) \implies b * e = c * e \implies b = c,$$

a contradiction again. The figure below shows both cases.

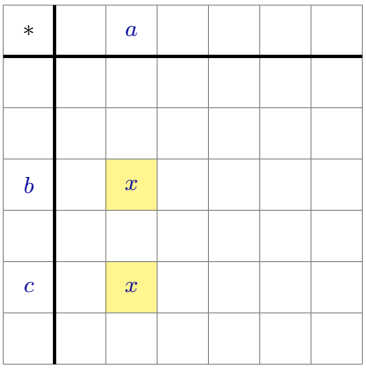
The two results are **cancellation**: from $a * b = a * c$ conclude $b = c$, and from $b * a = c * a$ conclude $b = c$. The a being cancelled must be on the same side in both products. $a * b = c * a$ does not give $b = c$ unless the group is abelian.

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:



a repeat in a row: $a * b = a * c$
impossible unless $b = c$



a repeat in a column: $b * a = c * a$
impossible unless $b = c$

Figure 7: 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.

- **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[53], 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[54]). 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.

[53] courses/math1061/practice-problems.pdf
[54] courses/math1061/subgroups-and-cyclic-groups.pdf

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[55]. The same works in a non-abelian group. In S_3, list f_1, f_5, f_6 first:

$\{f_1, f_5, f_6\}$ is every power of f_5, since $f_5^2 = f_6$ and $f_5^3 = f_1$, so it is the cyclic subgroup $\langle f_5 \rangle$ (symmetric-group[56]).

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[57]
$(S_3, \circ)$	6	**no**	2026-09-24-definitions-and-examples-of-groups[58]
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	4	yes	practice-problems[59], Q4; above
$(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$	4	yes	the same practice set, Q5
$(\mathbb{Z}_3, +)$	3	yes	integers-modulo-n[60]

[55] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[56] courses/math1061/symmetric-group.pdf
[57] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[58] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[59] courses/math1061/practice-problems.pdf
[60] courses/math1061/integers-modulo-n.pdf

Group	Elements	Abelian?	Where
$(\mathbb{Z}_6, +)$, even classes first	6	yes	2026-10-06-elementary-properties-of-groups[61]
$(S_3, \circ)$, f_1, f_5, f_6 first	6	**no**	above

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

Common mistakes

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

See also

- [groups] — the four properties the table is checked against, and cancellation as solving $a * x = b$
- integers-modulo-n[62] — the groups $\mathbb{Z}_n$ and $\mathbb{Z}_n - \{[0]\}$ behind the first tables
- symmetric-group[63] — S_3, whose table is not symmetric
- subgroups-and-cyclic-groups[64] — subgroups and cyclic subgroups, the blocks found above
- proof-techniques[65] — proof by contradiction, the method of the rows result
- 2026-09-24-definitions-and-examples-of-groups[66] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[67] — Lecture 27 · 2026-10-08-definitions-and-examples-of-fields[68] — Lecture 28, where the table of $\mathbb{Z}_4 - \{[0]\}$ fails closure

[61] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[62] courses/math1061/integers-modulo-n.pdf
[63] courses/math1061/symmetric-group.pdf
[64] courses/math1061/subgroups-and-cyclic-groups.pdf
[65] courses/math1061/proof-techniques.pdf
[66] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[67] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[68] courses/math1061/2026-10-08-definitions-and-examples-of-fields.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 8: 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.

- practice-problems[69] — §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[70]; the properties are defined in one-to-one-and-onto-functions[71] and inverse-functions[72].

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
>
> $$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in X.$$

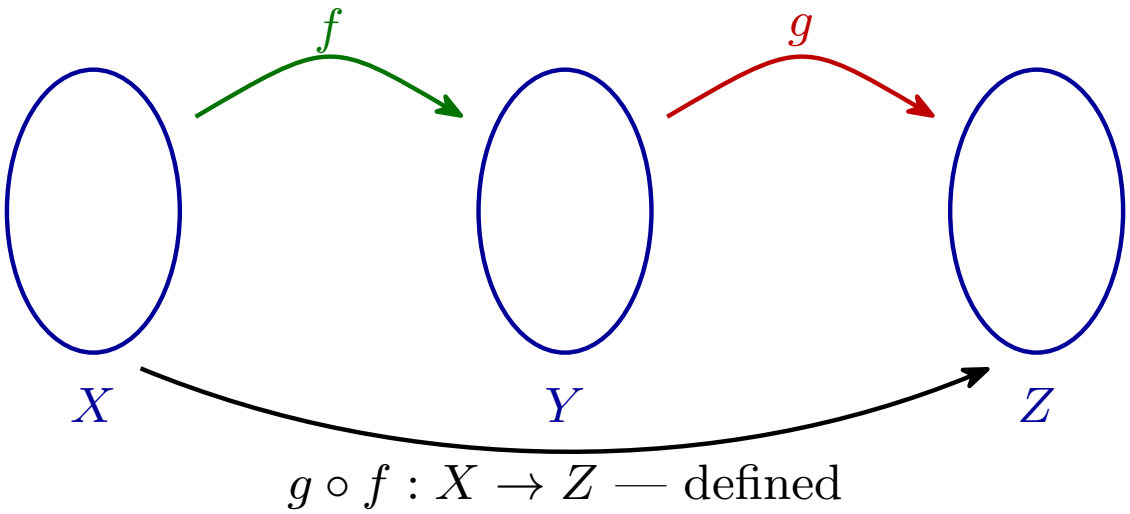
Three things to read off the definition:

- **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[73]: 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 $(f \circ g)(x) = 2x + 1$.

[69] courses/math1061/practice-problems.pdf
[70] courses/math1061/2026-09-08-composition-of-functions.pdf
[71] courses/math1061/one-to-one-and-onto-functions.pdf
[72] courses/math1061/inverse-functions.pdf
[73] courses/math1061/2026-09-08-composition-of-functions.pdf



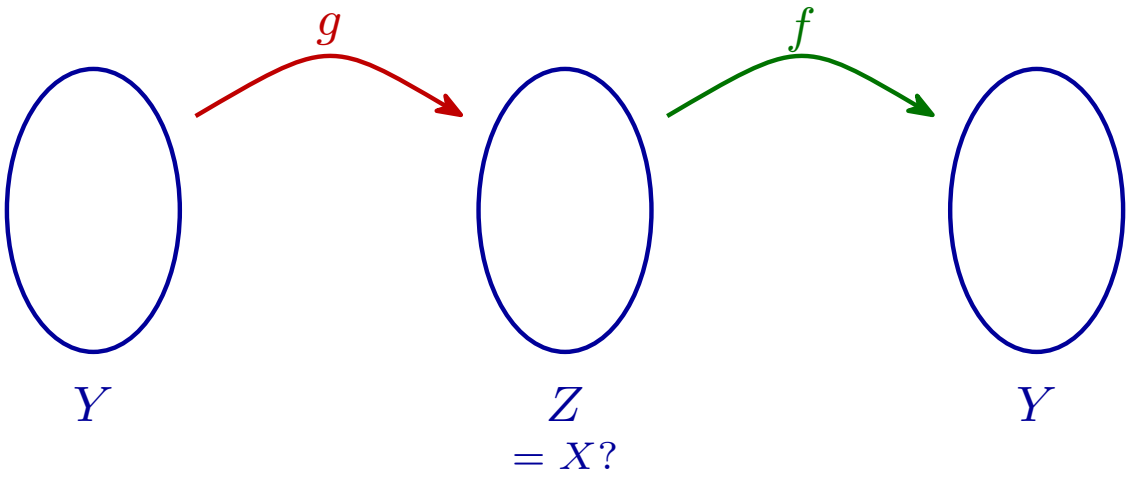


Figure 9: Why $g \circ f$ exists and $f \circ g$ usually does not. Top: f then g chains because f lands exactly where g starts. Bottom: g then f would need g's outputs, in Z, to be acceptable inputs to f, which come from X — so it is defined only if $Z = X$.

Inverses and composition

For a bijection $f : X \to Y$ with inverse $f^{-1} : Y \to X$ (inverse-functions[74]), 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, $x_1 = x_2$. $\square$

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.

[74] courses/math1061/inverse-functions.pdf

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. $\square$

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. $\square$

Both go by contraposition (proof-techniques[75]) 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.

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[76], 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.

[75] courses/math1061/proof-techniques.pdf
[76] courses/math1061/2026-09-08-composition-of-functions.pdf

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[77] — the properties and their proof templates
- inverse-functions[78] — $f \circ f^{-1}$ as the identity
- symmetric-group[79] — composition as the operation of a group, on the bijections of $\{1, \dots, n\}$
- groups[80] — the functions $ax+b$ with $a \neq 0$, a second non-abelian group under composition
- proof-techniques[81] — contraposition and counterexample
- 2026-09-08-composition-of-functions[82] — Lecture 20 · 2026-09-07-functions-one-to-one-onto-inverse[83] — Lecture 19
- practice-problems[84] — §26

Fields

A field is a set with two operations, $+$ and $\cdot$, in which you can add, subtract, multiply, and divide by anything except 0, with all the usual rules holding. Formally it is two abelian [groups] on one set, $(F, +)$ on all of it and $(F - \{0\}, \cdot)$ on everything but 0, tied together by the distributive laws. $\mathbb{Q}$ and $\mathbb{R}$ are fields, $\mathbb{Z}$ is not, and $\mathbb{Z}_n$ (integers-modulo-n[85]) is a field exactly when n is prime. In a field every linear equation $ax + b = c$ with $a \neq 0$ has exactly one solution. First met in 2026-10-08-definitions-and-examples-of-fields[86].

The definition

> **Definition.** A **field** $(F, +, \cdot)$ is a set F with two binary operations $+$ and $\cdot$ such that
>
> **(1)** $(F, +)$ is an abelian group;
>
> **(2)** $(F - \{0\}, \cdot)$ is an abelian group, where 0 is the identity of $(F, +)$; and

[77] courses/math1061/one-to-one-and-onto-functions.pdf
[78] courses/math1061/inverse-functions.pdf
[79] courses/math1061/symmetric-group.pdf
[80] courses/math1061/groups.pdf
[81] courses/math1061/proof-techniques.pdf
[82] courses/math1061/2026-09-08-composition-of-functions.pdf
[83] courses/math1061/2026-09-07-functions-one-to-one-onto-inverse.pdf
[84] courses/math1061/practice-problems.pdf
[85] courses/math1061/integers-modulo-n.pdf
[86] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

(3) for all $f, g, h \in F$, $f \cdot (g + h) = (f \cdot g) + (f \cdot h)$ and $(f + g) \cdot h = (f \cdot h) + (g \cdot h)$.

Written out, conditions (1) and (2) are five checks each, side by side:

	Addition, on F	Multiplication, on $F - \{0\}$
closure	$f + g \in F$	$f, g \neq 0 \Rightarrow f \cdot g \neq 0$
associativity	$(f + g) + h = f + (g + h)$	$(f \cdot g) \cdot h = f \cdot (g \cdot h)$
identity	0, with $0 + f = f + 0 = f$	1, with $1 \cdot f = f \cdot 1 = f$
inverses	every f has $-f$, with $f + (-f) = 0$	every $f \neq 0$ has f^{-1}, with $f \cdot f^{-1} = 1$
commutativity	$f + g = g + f$	$f \cdot g = g \cdot f$

Condition (3) is the two distributive laws, which hold for all $f, g, h \in F$, zero included.

Points that are easy to read past:

- **The two identities are named 0 and 1 by their jobs,** not because they are the integers 0 and 1. In $\mathbb{Z}_n$ they are [0] and [1]. The "0" removed in condition (2) is whatever the additive identity is.
- **Closure in (2) is a real condition.** It says that a product of two non-zero elements is never 0. It is the condition $\mathbb{Z}_4$ and $\mathbb{Z}_{15}$ fail.
- **$-f$ and f^{-1} are different inverses.** Each element has an additive inverse, and each non-zero element has a multiplicative one as well. In $\mathbb{Z}_5$, $-[2] = [3]$ and $[2]^{-1} = [3]$ happen to agree, but $-[4] = [1]$ while $[4]^{-1} = [4]$.
- **The distributive laws are the only link between the operations.** Without (3), a field would be two unrelated groups that happen to share a set.

Why 0 is left out of (2). In any field, $0 \cdot f = 0$ for every f. By the distributive law,

$$0 \cdot f = (0 + 0) \cdot f = (0 \cdot f) + (0 \cdot f),$$

and adding $-(0 \cdot f)$ to both sides leaves $0 = 0 \cdot f$. So $0 \cdot y = 1$ has no solution, and 0 can never have a multiplicative inverse. Asking for a group on all of F under $\cdot$ would rule out every field, just as 0 stops $(\mathbb{R}, \cdot)$ being a group (groups[87]).

Examples and non-examples

[87] courses/math1061/groups.pdf

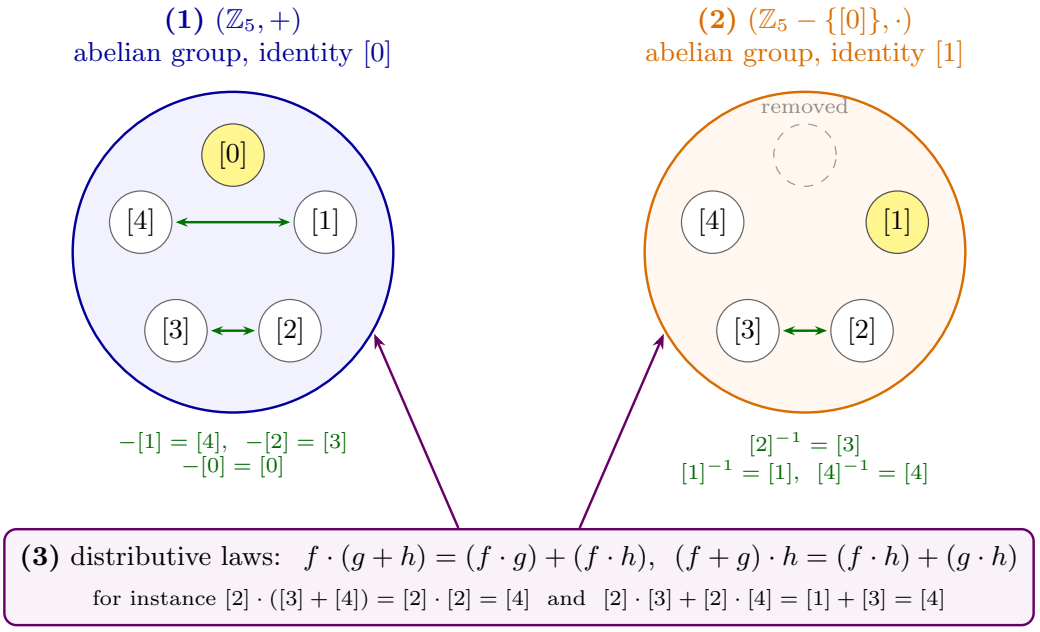


Figure 10: A field is two abelian groups on one set, shown for $\mathbb{Z}_5$. Left: all five classes under addition, identity [0]. A line joins each class to its additive inverse; [0] is its own. Right: the same classes under multiplication, with [0] taken out and identity [1]. [2] and [3] are inverses, and [1] and [4] are their own. The same class can have different inverses in the two groups: $-[4] = [1]$ but $[4]^{-1} = [4]$. Below: the distributive laws, the one condition that mentions both operations, checked on one instance.

	Field?	Why
$(\mathbb{Q}, +, \cdot)$	**yes**	every non-zero $\frac{a}{b}$ has inverse $\frac{b}{a}$
$(\mathbb{R}, +, \cdot)$	**yes**	every non-zero x has inverse $\frac{1}{x}$
$(\mathbb{Z}, +, \cdot)$	**no**	2 has no multiplicative inverse in $\mathbb{Z}$
$(\mathbb{Z}_7, +, \cdot)$	**yes**	7 is prime
$(\mathbb{Z}_4, +, \cdot)$	**no**	$[2] \cdot [2] = [0]$: closure fails in (2)
$(\mathbb{Z}_{15}, +, \cdot)$	**no**	$[3] \cdot [5] = [0]$: closure fails in (2)
$(\mathbb{Z}_{12}, +, \cdot)$	**no**	$[2]$ has no inverse, since $2k$ is even and never $\equiv 1 \pmod{12}$

$\mathbb{Z}$, $\mathbb{Z}_4$, $\mathbb{Z}_7$ and $\mathbb{Z}_{15}$ are worked in 2026-10-08-definitions-and-examples-of-fields[88] and 2026-10-08-definitions-and-examples-of-fields[89]. $\mathbb{Z}_{12}$ is Q2 of practice-problems[90], and Q3 of the same set checks every condition for an unfamiliar field on $\mathbb{Q} \times \mathbb{Q}$.

Every one of the non-examples passes (1) and (3) and fails (2). That is the usual pattern: addition is rarely the problem, and the work in deciding whether something is a field is in the multiplicative group.

To show something is not a field, one failure with specific elements is enough, as for groups: "2 has no inverse in $\mathbb{Z}$", or "$[3] \cdot [5] = [0]$ in $\mathbb{Z}_{15}$".

$\mathbb{Z}_n$ is a field exactly when n is prime

> $(\mathbb{Z}_n, +)$ **is a group for every** $n \in \mathbb{Z}^+$**.**
> $(\mathbb{Z}_p, +, \cdot)$ **is a field when** p **is prime.**

For any n, condition (1) holds (integers-modulo-n[91]), and condition (3), associativity, commutativity and the identity $[1]$ for multiplication are all inherited from the integers, for example $[a]([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c]$. So whether $\mathbb{Z}_n$ is a field comes down to two things about $\mathbb{Z}_n - \{[0]\}$: is it **closed** under multiplication, and does every class in it have an **inverse**?

[88] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[89] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[90] courses/math1061/practice-problems.pdf
[91] courses/math1061/integers-modulo-n.pdf

When n is composite, closure fails. Write $n = rs$ with $1 < r, s < n$. Then $[r]$ and $[s]$ are non-zero, but

$$[r] \cdot [s] = [rs] = [n] = [0].$$

$\mathbb{Z}_4$ $(2 \cdot 2)$, $\mathbb{Z}_6$ $(2 \cdot 3)$, $\mathbb{Z}_{12}$ $(3 \cdot 4)$ and $\mathbb{Z}_{15}$ $(3 \cdot 5)$ all fail this way. A non-zero class that multiplies something non-zero into $[0]$ also has no inverse: if $[a][b] = [0]$ with $[b] \neq [0]$, multiplying both sides by an inverse of $[a]$ would give $[b] = [0]$. That is why $[2]$, with $[2][6] = [0]$, has no inverse in $\mathbb{Z}_{12}$.

When $n = p$ is prime, both hold.

- *Closure.* If $[a] \cdot [b] = [0]$ then $p \mid ab$. The prime p appears in the prime factorisation of ab, which is the factorisation of a together with that of b (divisibility-and-factorisation[92]), so $p \mid a$ or $p \mid b$. That is, $[a] = [0]$ or $[b] = [0]$. A product of non-zero classes is non-zero.
- *Inverses.* Fix $[a] \neq [0]$ and look at its row of the table, $[a][1], [a][2], \ldots, [a][p-1]$. By closure none of these is $[0]$. No two are equal: if $[a][b] = [a][c]$ then $p \mid a(b-c)$, and since $p \nmid a$, the same argument gives $p \mid (b-c)$, so $[b] = [c]$. That is $p - 1$ different non-zero classes, which is all of them, so one of them is $[1]$. Whichever $[b]$ gives it is $[a]^{-1}$.

So $\mathbb{Z}_n$ is a field for $n = 2, 3, 5, 7, 11, 13, \ldots$ and for no other $n \geq 2$. ($\mathbb{Z}_1$ has one class, $\mathbb{Z}_1 - \{[0]\}$ is empty, and the empty set has no identity, so it is not a field either.)

$\mathbb{Z}_5 - \{[0]\}$: closed, every row has $[1]$

$\cdot$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	**(1)**	$[2]$	$[3]$	$[4]$
$[2]$	$[2]$	$[4]$	**(1)**	$[3]$
$[3]$	$[3]$	**(1)**	$[4]$	$[2]$
$[4]$	$[4]$	$[3]$	$[2]$	**(1)**

$\mathbb{Z}_6 - \{[0]\}$: not closed

$\cdot$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	
$[1]$	**(1)**	$[2]$	$[3]$	$[4]$	$[5]$	
$[2]$	$[2]$	$[4]$	**[0]**	$[2]$	$[4]$	no [1]
$[3]$	$[3]$	**[0]**	$[3]$	**[0]**	$[3]$	no [1]
$[4]$	$[4]$	$[2]$	**[0]**	$[4]$	$[2]$	no [1]
$[5]$	$[5]$	$[4]$	$[3]$	$[2]$	**(1)**	

Figure 11: Multiplication on the non-zero classes of $\mathbb{Z}_5$ and of $\mathbb{Z}_6$. Left, $p = 5$ prime: no product is $[0]$, so the set is closed, and $[1]$ (ringed) appears once in every row and every column, so every class has an inverse. Right, $n = 6 = 2 \cdot 3$: the red cells are products of two non-zero classes that come out as $[0]$, so closure fails. The rows of $[2]$, $[3]$ and $[4]$, the classes sharing a factor with 6, contain no $[1]$, so those classes have no inverse. Only $[1]$ and $[5]$ do.

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

Calculating in a field

The two inverses give the other two operations:

- **Subtraction** is adding the additive inverse: $f - g = f + (-g)$.
- **Division** is multiplying by the multiplicative inverse: $f \div g = f \cdot g^{-1}$, for $g \neq 0$.

In $\mathbb{Q}$ and $\mathbb{R}$ these are the familiar operations. In $\mathbb{Z}_p$:

- $-[a] = [-a] = [p - a]$. In $\mathbb{Z}_{11}$, $-[3] = [8]$, because $[3] + [8] = [11] = [0]$.
- $[a]^{-1}$ is the class $[b]$ with $ab \equiv 1 \pmod{p}$. It is never a fraction: in $\mathbb{Z}_{11}$, $[2]^{-1} = [6]$, because $2 \cdot 6 = 12 \equiv 1$. Ways to find it are in integers-modulo-n[93].

So "$5 \div 2$" in $\mathbb{Z}_{11}$ is $[5] \cdot [6] = [30] = [8]$, and indeed $[2] \cdot [8] = [16] = [5]$.

Solving linear equations

To solve $ax + b = c$ in a field, with $a \neq 0$:

1. **Add $-b$ to both sides**, which exists by (1): $ax = c + (-b)$.
2. **Multiply both sides by a^{-1}**, which exists by (2) because $a \neq 0$: $x = a^{-1} \cdot (c + (-b))$.
3. **Check** by substituting back.

Each step is reversible, since b and a can be put back by adding b and multiplying by a. So the equation has **exactly one solution**, $x = a^{-1}(c - b)$. It is the two-group version of solving $a * x = b$ in a group (groups[94]).

Worked: an equation in $\mathbb{Z}_{13}$

Solve $5x + 7 = 3$ in the field $(\mathbb{Z}_{13}, +, \cdot)$.

$$\begin{aligned} 5x + 7 &= 3 \\ 5x &= 3 + (-7) = -4 = 9 && \text{add } -7 \\ 8 \cdot 5x &= 8 \cdot 9 && [5]^{-1} = [8], \text{ since } 5 \cdot 8 = 40 = 3 \cdot 13 + 1 \\ x &= 72 = 7 && 72 = 5 \cdot 13 + 7 \end{aligned}$$

Check: $5 \cdot 7 + 7 = 42 = 3 \cdot 13 + 3 \equiv 3 \pmod{13}$. ✓ So $x = [7]$.

With a bracket, multiply by the inverse first. For $3(x + 2) = 5$ in $\mathbb{Z}_7$: $[3]^{-1} = [5]$, so $x + 2 = 5 \cdot 5 = 25 = 4$, and $x = 4 - 2 = [2]$. *Check:* $3(2 + 2) = 12 \equiv 5 \pmod{7}$. Expanding with the distributive law first, $3x + 6 = 5$, gives the same answer by the usual two steps.

[93] courses/math1061/integers-modulo-n.pdf
[94] courses/math1061/groups.pdf

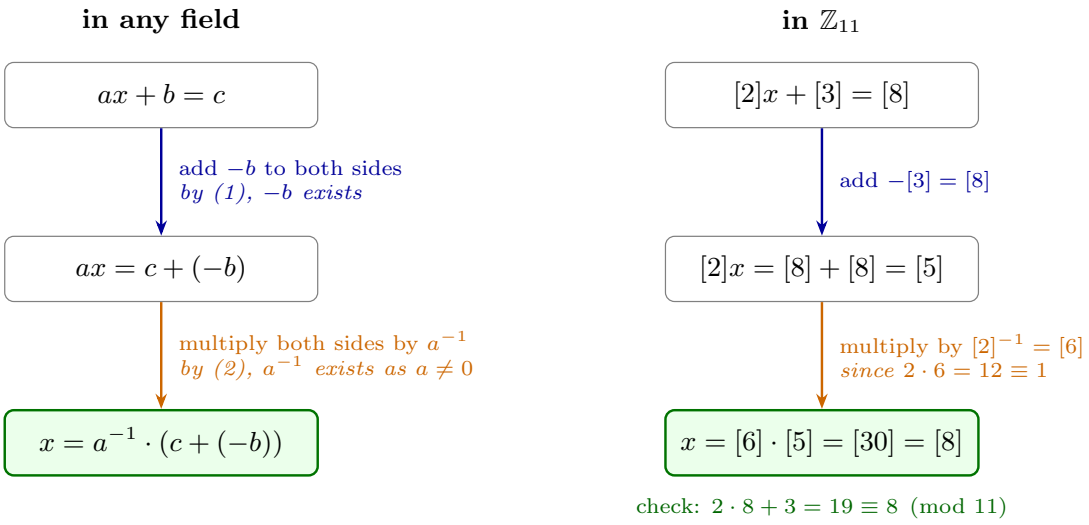


Figure 12: Solving $ax + b = c$ in a field, on the left in general and on the right for $2x + 3 = 8$ in $\mathbb{Z}_{11}$. Each arrow applies one inverse to both sides. The first uses the additive group, condition (1): every element, here [3], has a negative, $[-3] = [8]$. The second uses the multiplicative group, condition (2): every non-zero element, here [2], has an inverse, [6]. Neither step can fail in a field, so the equation always has exactly one solution.

The two equations of 2026-10-08-definitions-and-examples-of-fields[95] are worked the same way: $2x + 3 = 8$ in $\mathbb{Z}_{11}$ gives $x = [8]$, and $10x + 9 = 6$ in $\mathbb{Z}_{17}$ gives $x = [15]$. More are in practice-problems[96], Q1.

From a class to an integer

A solution in $\mathbb{Z}_p$ is a class, and the integers y satisfying the matching congruence are exactly the members of that class. For $2y + 3 \equiv 8 \pmod{11}$ they are $[8] = \{\dots, -3, 8, 19, \dots\}$. The **smallest positive** one is the usual representative of the class when that is between 1 and $p - 1$, and p itself when the solution is $[0]$. In the column picture of integers-modulo-n[97] it is the shaded entry of the column, or the entry just below it for $[0]$. A negative representative, such as -2 for $[15]$ in $\mathbb{Z}_{17}$, names the right class but is not the positive integer asked for.

When the set is not a field

In $\mathbb{Z}_{15}$, $[3]$ has no inverse, and the method breaks in both possible ways:

- $3x = 5$ has **no** solution, because $3x$ is always one of $[0], [3], [6], [9], [12]$;
- $3x = 6$ has **three**, $x = [2], [7], [12]$.

Exactly one solution for every $a \neq 0$ is what being a field buys.

Common mistakes

- **Checking only addition.** $(F, +)$ is usually the easy part. The work is in $(F - \{0\}, \cdot)$, and that is where $\mathbb{Z}$, $\mathbb{Z}_4$ and $\mathbb{Z}_{15}$ fail.
- **Asking 0 for a multiplicative inverse,** or forgetting to remove it. Condition (2) is about $F - \{0\}$.
- **Assuming every $\mathbb{Z}_n$ is a field.** Only prime n works. For composite n, removing $[0]$ is not enough, because other products land on $[0]$.
- **Leaving a fraction in $\mathbb{Z}_p$.** $2x = 5$ in $\mathbb{Z}_{11}$ does not give $x = \frac{5}{2}$. It gives $x = [6][5] = [8]$.
- **Using the wrong inverse.** To clear "+3" add $-[3]$; to clear "2·" multiply by $[2]^{-1}$. In $\mathbb{Z}_{11}$ these are $[8]$ and $[6]$, different classes.
- **Not reducing the answer.** $x = [-36]$ in $\mathbb{Z}_{17}$ is correct but unfinished: it is $[15]$. If a question wants the smallest positive integer, a negative representative is not it.
- **Skipping the check.** Substituting back takes one line and catches an inverse found wrongly.
- **Forgetting the distributive laws** when checking an unfamiliar structure. They are a separate condition, and two groups on one set without them are not a field.

[95] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[96] courses/math1061/practice-problems.pdf
[97] courses/math1061/integers-modulo-n.pdf

See also

- [groups] — the four properties behind conditions (1) and (2), and solving $a * x = b$
- integers-modulo-n[98] — $\mathbb{Z}_n$, $\mathbb{Z}_p$, and finding multiplicative inverses mod p
- subgroups-and-cyclic-groups[99] — subgroups, $\langle a \rangle$, and cyclic groups
- divisibility-and-factorisation[100] — unique factorisation, used for why $\mathbb{Z}_p$ is a field
- cayley-tables[101] — reading closure and inverses off a table
- 2026-10-08-definitions-and-examples-of-fields[102] — Lecture 28
- practice-problems[103] — §36, 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[104], and the bijections of the symmetric-group[105] under composition. A small group is checked from its table (cayley-tables[106]). Groups inside groups, and the powers of an element, are in subgroups-and-cyclic-groups[107]. First met in 2026-09-24-definitions-and-examples-of-groups[108], and continued in 2026-10-06-elementary-properties-of-groups[109].

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

[98] courses/math1061/integers-modulo-n.pdf
[99] courses/math1061/subgroups-and-cyclic-groups.pdf
[100] courses/math1061/divisibility-and-factorisation.pdf
[101] courses/math1061/cayley-tables.pdf
[102] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[103] courses/math1061/practice-problems.pdf
[104] courses/math1061/integers-modulo-n.pdf
[105] courses/math1061/symmetric-group.pdf
[106] courses/math1061/cayley-tables.pdf
[107] courses/math1061/subgroups-and-cyclic-groups.pdf
[108] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[109] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

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[110]).
- **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.

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 $(g \circ f)(x) = 2x + 1$

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

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[111]).

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.

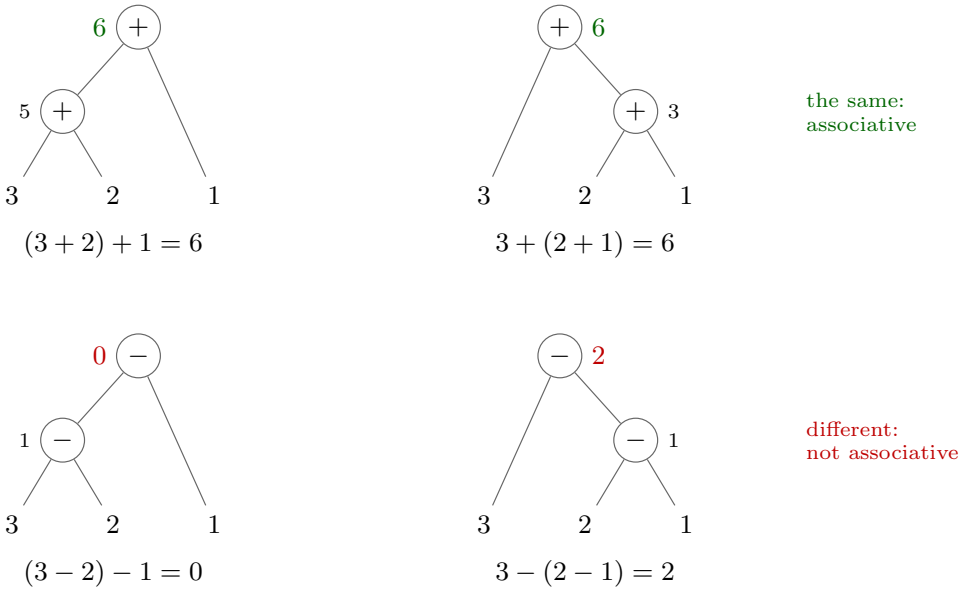


Figure 13: The two ways of bracketing three elements, drawn as trees: the lower operation is done first, and its result feeds the upper one. Top row, addition: both bracketings of $3 + 2 + 1$ give 6. Addition is associative, so the brackets can be dropped. Bottom row, subtraction: $(3 - 2) - 1 = 0$ and $3 - (2 - 1) = 2$. The same three numbers in the same order give different answers, so subtraction is not associative and $(\mathbb{Z}, -)$ is not a group.

Operation	Associative	Commutative
$+$ and $\cdot$ on numbers	yes	yes

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

Operation	Associative	Commutative
$\circ$ 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.
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[112], 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: $1 \star x = 1 + x - 1 = x$.

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

- **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[113])? All eight against all four properties:

	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[114]: $[1]^{-1} = [1]$, $[2]^{-1} = [3]$, $[3]^{-1} = [2]$, $[4]^{-1} = [4]$.

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[115].

[113] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[114] courses/math1061/practice-problems.pdf
[115] courses/math1061/integers-modulo-n.pdf

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[116]). 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)
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:

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

- **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[117], proved in 2026-09-24-definitions-and-examples-of-groups[118]).
- **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.

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.

$$(g * h)^{-1} = h^{-1} * g^{-1}.$$

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

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.

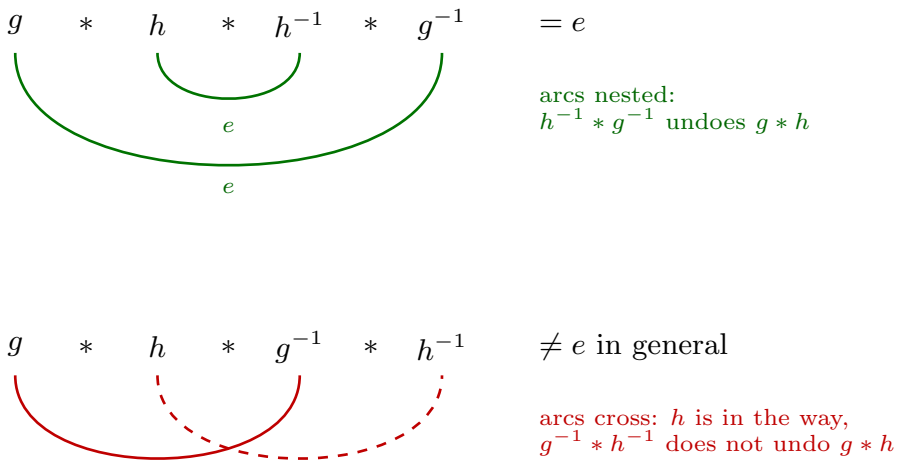


Figure 14: Why the inverse of $g * h$ is $h^{-1} * g^{-1}$ and not $g^{-1} * h^{-1}$. Top: in $g * h * h^{-1} * g^{-1}$ each element sits next to its inverse once the inner pair is gone. The inner arc, $h * h^{-1} = e$, cancels first, and that brings g next to g^{-1}, so the whole product is e. The arcs 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.

A check in S_3 (symmetric-group[119]). $f_2 \circ f_3 = f_6$, 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 $f_2^{-1} \circ f_3^{-1} = f_2 \circ f_3 = f_6$, 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.

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

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[120]).

The inverse facts are Q2 of practice-problems[121].

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[122] — a finite group as a table, and what can be read off it
- integers-modulo-n[123] — $\mathbb{Z}_n$ under addition, and $\mathbb{Z}_n - \{[0]\}$ under multiplication
- symmetric-group[124] — the group of bijections of $\{1, \ldots, n\}$, the course's non-abelian example
- subgroups-and-cyclic-groups[125] — subgroups, powers of an element, cyclic subgroups and cyclic groups
- [fields] — two abelian groups on one set, under $+$ and under $\cdot$, joined by the distributive laws
- composition-of-functions[126] — the operation of S_n and of the group of functions $ax + b$

[120] courses/math1061/subgroups-and-cyclic-groups.pdf
[121] courses/math1061/practice-problems.pdf
[122] courses/math1061/cayley-tables.pdf
[123] courses/math1061/integers-modulo-n.pdf
[124] courses/math1061/symmetric-group.pdf
[125] courses/math1061/subgroups-and-cyclic-groups.pdf
[126] courses/math1061/composition-of-functions.pdf

- quantified-statements[127] — the two orders of quantifiers in the identity and inverse properties
- proof-techniques[128] — direct proof and counterexample, the methods the checks use
- 2026-09-24-definitions-and-examples-of-groups[129] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[130] — Lecture 27
- practice-problems[131] — §33, with full worked solutions · practice-problems[132] — §34

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[133], and equivalence classes in equivalence-classes-and-partitions[134]. Under addition $\mathbb{Z}_n$ is one of the course's standard [groups], and when n is prime it is a field, with division by every non-zero class ([fields]). First met in 2026-09-24-definitions-and-examples-of-groups[135].

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[136]), so every integer is in exactly one of the n classes.

[127] courses/math1061/quantified-statements.pdf
[128] courses/math1061/proof-techniques.pdf
[129] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[130] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[131] courses/math1061/practice-problems.pdf
[132] courses/math1061/practice-problems.pdf
[133] courses/math1061/modular-arithmetic.pdf
[134] courses/math1061/equivalence-classes-and-partitions.pdf
[135] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[136] courses/math1061/modular-arithmetic.pdf

- **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[137]).

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

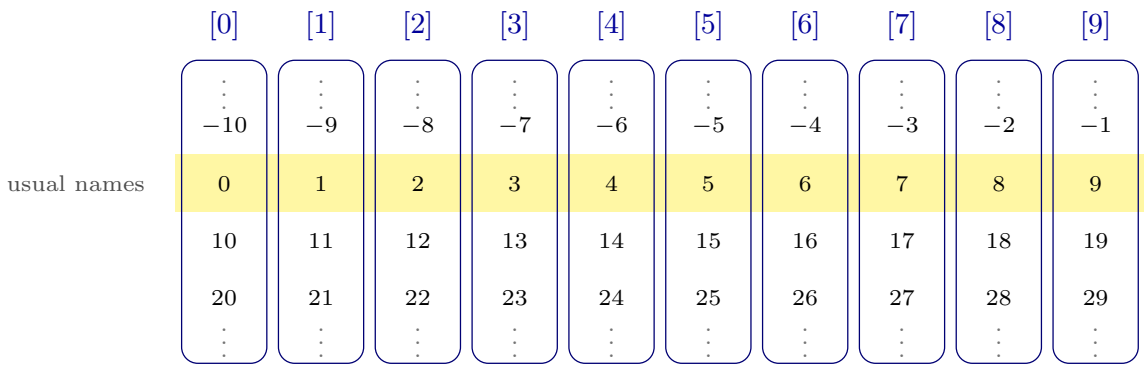


Figure 15: The integers from -10 to 29 written in rows of ten. Each column is one element of $\mathbb{Z}_{10}$: going down a column adds 10, so everything in a column is congruent mod 10. The whole of $\mathbb{Z}$ is sorted into these ten columns, and $\mathbb{Z}_{10}$ is the set of the ten columns. The shaded row holds the usual representatives, 0 to 9. Any other number in a column names the same class, so $[21] = [1]$ and $[-1] = [9]$.

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 $[8] \cdot [9] = [72] = [2]$.

Any representative can be used

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

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

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[138]: 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 $[ab]=[a'b']$.

+	−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 16: $[8]+[9]$ 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 $[8]\cdot[9]=[2]$.

Choosing a convenient representative

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

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

$[9]$ 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[139]):

[138] courses/math1061/modular-arithmetic.pdf
[139] courses/math1061/groups.pdf

- **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[140]:

$+$	$[0]$	$[1]$	$[2]$
$[\mathbf{0}]$	$[0]$	$[1]$	$[2]$
$[\mathbf{1}]$	$[1]$	$[2]$	$[0]$
$[\mathbf{2}]$	$[2]$	$[0]$	$[1]$

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[141]; table in practice-problems[142], Q4
$\mathbb{Z}_7 - \{[0]\}$	**yes**	2026-09-24-definitions-and-examples-of-groups[143]
$\mathbb{Z}_9 - \{[0]\}$	**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[144]

[140] courses/math1061/groups.pdf
[141] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[142] courses/math1061/practice-problems.pdf
[143] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[144] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

	Group under multiplication?	Worked in
$\mathbb{Z}_{15} - \{[0]\}$	**no**: not closed, $[3] \cdot [5] = [15] = [0]$	2026-10-08-definitions-and-examples-of-fields[145]

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[146].

$\mathbb{Z}_p$ is a field

$(\mathbb{Z}_p, +, \cdot)$ is a field when p is prime. All three conditions of fields[147] hold:

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[148]). 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[149]).

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[150], 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[151]: each non-zero number is joined to its inverse.

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

[145] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[146] courses/math1061/fields.pdf
[147] courses/math1061/fields.pdf
[148] courses/math1061/fields.pdf
[149] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[150] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[151] courses/math1061/2026-09-17-relations-reflexivity-symmetry-transitivity.pdf

- **List the multiples.** Write $a, 2a, 3a, \ldots \bmod p$, 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[152]. 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]	$[2] \leftrightarrow [3]$
7	[1], [6]	$[2] \leftrightarrow [4]$, $[3] \leftrightarrow [5]$
11	[1], [10]	$[2] \leftrightarrow [6]$, $[3] \leftrightarrow [4]$, $[5] \leftrightarrow [9]$, $[7] \leftrightarrow [8]$

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.

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[153]): 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[154]).

[152] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[153] courses/math1061/sets-and-set-notation.pdf
[154] courses/math1061/modular-arithmetic.pdf

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[155] — congruence, remainders, and the lemma that makes class arithmetic work
- equivalence-classes-and-partitions[156] — classes and representatives in general
- [groups] — the definition $\mathbb{Z}_n$ is checked against
- [fields] — why $\mathbb{Z}_n$ is a field exactly when n is prime, and solving equations in $\mathbb{Z}_p$
- subgroups-and-cyclic-groups[157] — cyclic subgroups and cyclic groups; $(\mathbb{Z}_n, +)$ is cyclic, generated by $[1]$
- cayley-tables[158] — 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[159] — Lecture 26 · 2026-09-21-equivalence-relations[160] — Lecture 24, where the classes of congruence mod 3 are drawn
- 2026-10-06-elementary-properties-of-groups[161] — 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[162] — 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[163] — §33, with full worked solutions
- practice-problems[164] — §36, equations in $\mathbb{Z}_5$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$ and $\mathbb{Z}_{19}$

[155] courses/math1061/modular-arithmetic.pdf
[156] courses/math1061/equivalence-classes-and-partitions.pdf
[157] courses/math1061/subgroups-and-cyclic-groups.pdf
[158] courses/math1061/cayley-tables.pdf
[159] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[160] courses/math1061/2026-09-21-equivalence-relations.pdf
[161] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[162] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[163] courses/math1061/practice-problems.pdf
[164] courses/math1061/practice-problems.pdf

Inverse Functions

When a function can be run backwards, what the backwards function is, and the one notational trap: f^{-1} **means two different things**, and the braces tell you which. Builds on one-to-one-and-onto-functions[165]; the preimage half is from functions-on-general-sets[166]; the lecture is 2026-09-07-functions-one-to-one-onto-inverse[167].

Bijections have inverses

A function that is both one-to-one and onto is said to be a **bijection**.

A bijection $f : X \to Y$ has an **inverse function** $f^{-1} : Y \to X$, where for all $y \in Y$,

$$f^{-1}(y) = x \text{ where } x \text{ is the unique } x \in X \text{ such that } f(x) = y.$$

Note the direction: $f : X \to Y$ **gives** $f^{-1} : Y \to X$. The inverse's domain is f's co-domain and vice versa.

The definition is exactly one sentence, and both properties are inside it:

- "x *… such that* $f(x) = y$" — such an x **exists** for every y because f is **onto**.
- "*the unique* x" — there is only **one** because f is **one-to-one**.

Drop either and f^{-1} is not a function: if f is not onto, some y has nowhere to go; if f is not one-to-one, some y has two places to go. Both failures are drawn in 2026-09-07-functions-one-to-one-onto-inverse[168]. And the converse holds too:

$$f \text{ has an inverse} \iff f \text{ is a bijection.}$$

Finding the inverse

The onto proof computes it. Proving f onto means taking an arbitrary y (or (a, b)) and producing the x that maps to it, as a formula in y. That formula is f^{-1}. It is a function whether or not f is one-to-one; one-to-one is what makes it the *inverse*, by guaranteeing the x it produces is the only preimage, so that $f^{-1} \circ f$ is the identity and not merely $f \circ f^{-1}$.

$f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $f((x, y)) = (y + 1, 2x)$ — a bijection (proved in one-to-one-and-onto-functions[169]).

[165] courses/math1061/one-to-one-and-onto-functions.pdf
[166] courses/math1061/functions-on-general-sets.pdf
[167] courses/math1061/2026-09-07-functions-one-to-one-onto-inverse.pdf
[168] courses/math1061/2026-09-07-functions-one-to-one-onto-inverse.pdf
[169] courses/math1061/one-to-one-and-onto-functions.pdf

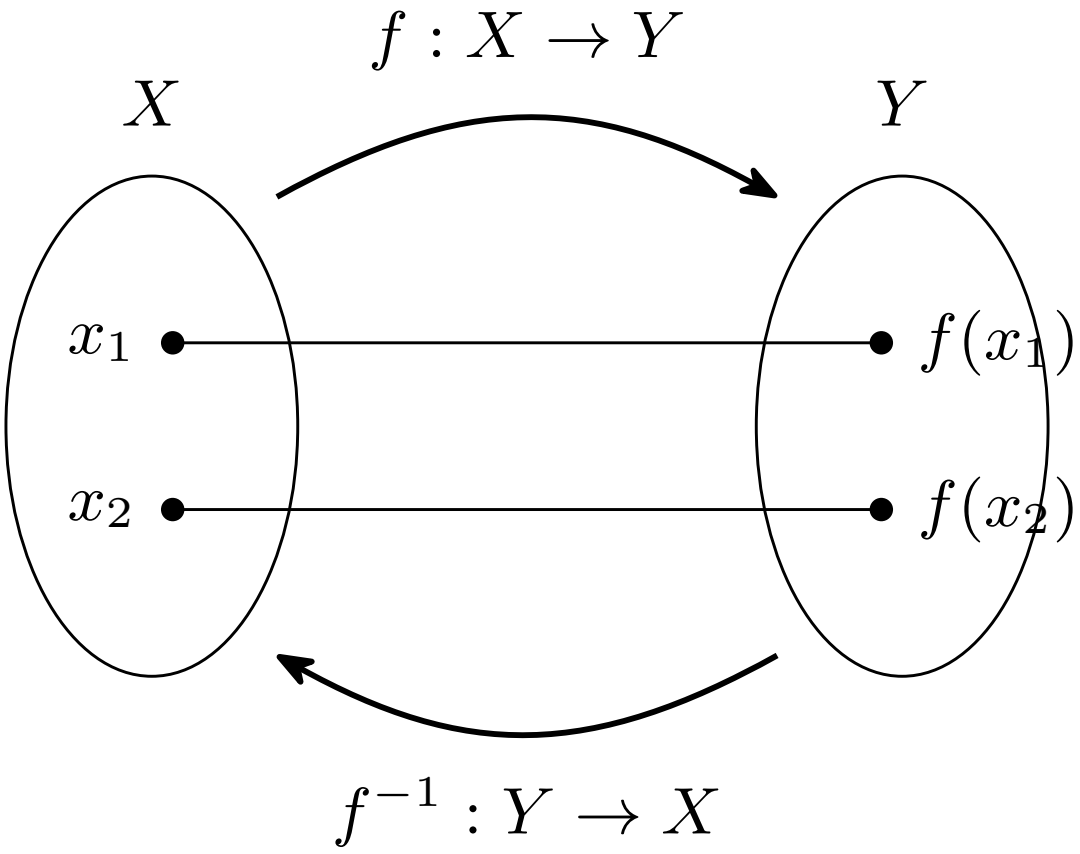


Figure 17: A bijection f pairs x_1 with $f(x_1)$ and x_2 with $f(x_2)$, one arrow each, nothing shared, nothing missed — and so the arrows can be read backwards. The curved arrow above is $f : X \to Y$; the one below is $f^{-1} : Y \to X$, the same pairs in the other direction.

The onto proof took, for (a, b), the candidate $\left(\frac{b}{2}, a-1\right)$. So

$$f^{-1} : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}, \qquad f^{-1}((a,b)) = \left(\tfrac{b}{2},\ a-1\right), \quad \text{i.e.} \quad f^{-1}((x,y)) = \left(\tfrac{y}{2},\ x-1\right).$$

Sense check, both ways:

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

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

In the language of composition-of-functions[170]: $f \circ f^{-1}$ and $f^{-1} \circ f$ are both the identity, and checking one of them is the standard way to confirm an inverse has been computed correctly.

For a function given by a formula in one variable the procedure is the same: set $f(x) = y$, solve for x in terms of y, and the solution is $f^{-1}(y)$ — provided the solution is unique and always in the domain, which is what "bijection" guarantees.

The two meanings of f^{-1}

This is the most common source of wrong answers in this topic.

> **1. Preimage.** If $f : X \to Y$ is **any** function and $A \subseteq Y$, then the **inverse image** or **preimage** of A is
> $$f^{-1}(A) = \{x \in X : f(x) \in A\}.$$
> The preimage function is a function $f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$.
>
> **2. Inverse function.** If $f : X \to Y$ is a **bijection**, then the **inverse function** of f is $f^{-1} : Y \to X$ with $f^{-1}(y) =$ the unique x such that $f(x) = y$. The inverse function is a function $f^{-1} : Y \to X$.

	Takes	Gives	Exists
preimage $f^{-1}(A)$	a **subset** $A \subseteq Y$	a **subset** of X	for **every** function
inverse function $f^{-1}(y)$	an **element** $y \in Y$	an **element** of X	only if f is a **bijection**

The braces decide. $f^{-1}(\{a\})$ has a set inside, so it is a preimage and always means something. $f^{-1}(a)$ has an element inside, so it is the inverse function and means something only if f is a bijection.

[170] courses/math1061/composition-of-functions.pdf

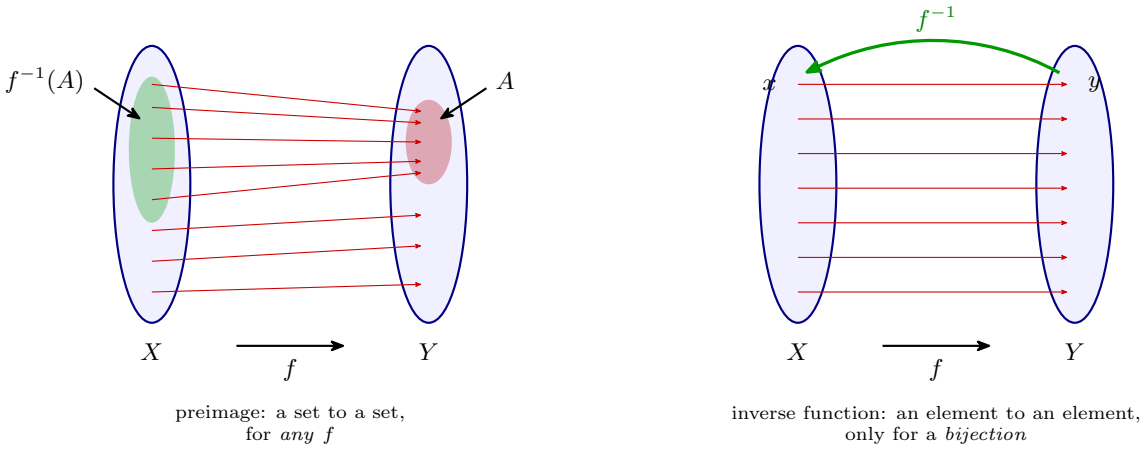


Figure 18: The two meanings side by side. Left: a many-to-one f, with a subset A of Y (red) and its preimage $f^{-1}(A)$ (green) — every x whose arrow lands in A. This exists for any function, and it is a set. Right: a bijective f, every arrow its own, and the single green arrow f^{-1} running one element back from y to x. Same symbol; the first eats sets and the second eats elements.

Worked: reading the braces

$$f : \{1, 2, 3, 4\} \to \{a, b, c\},\ f = \{(1, a), (2, a), (3, b), (4, b)\}.$$

f is not one-to-one ($1, 2 \mapsto a$) and not onto (c unreached), so it is not a bijection.

Statement		Because
The inverse function f^{-1} does not exist.	**T**	f is not a bijection
$f^{-1}(\{a\}) = \{1, 2\}$.	**T**	preimage: 1 and 2 map to a, nothing else does
$f^{-1}(a)$ is not defined.	**T**	a is an element, so this is the inverse function, which does not exist
$f^{-1}(\{c\}) = \emptyset$.	**T**	preimage: nothing maps to c, and $\emptyset$ is a perfectly good answer

All four are true. The second and third differ *only* in the braces, and one is a set while the other is undefined.

When f **is** a bijection the two meanings agree in the obvious way: $f^{-1}(\{y\}) = \{f^{-1}(y)\}$, a one-element set whose element is the inverse function's value. That is the only case in which it is safe to blur them, and even then the types differ.

See also

- one-to-one-and-onto-functions[171] — the two properties a bijection needs, and how to prove them
- composition-of-functions[172] — $f \circ f^{-1}$ and $f^{-1} \circ f$
- symmetric-group[173] — the inverse function as the inverse of an element of a group
- groups[174] — $f(x) = ax + b$ with $a \neq 0$ has inverse $f^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$, its inverse in the group of such functions
- functions-on-general-sets[175] — image and preimage, where meaning 1 comes from
- sets-and-set-notation[176] — power sets, which the preimage function maps between
- 2026-09-07-functions-one-to-one-onto-inverse[177] — Lecture 19 · 2026-09-08-composition-of-functions[178] — Lecture 20
- practice-problems[179] — §25

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[180]). 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

[171] courses/math1061/one-to-one-and-onto-functions.pdf
[172] courses/math1061/composition-of-functions.pdf
[173] courses/math1061/symmetric-group.pdf
[174] courses/math1061/groups.pdf
[175] courses/math1061/functions-on-general-sets.pdf
[176] courses/math1061/sets-and-set-notation.pdf
[177] courses/math1061/2026-09-07-functions-one-to-one-onto-inverse.pdf
[178] courses/math1061/2026-09-08-composition-of-functions.pdf
[179] courses/math1061/practice-problems.pdf
[180] courses/math1061/math1061.pdf

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:

- 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[181] 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[182]
2	Logical Equivalence	L2 (wk 1)	030–038	043–053	logical-equivalence-laws[183]

[181] courses/math1061/math1061.pdf
[182] courses/math1061/logical-connectives.pdf
[183] courses/math1061/logical-equivalence-laws.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
3	Conditional Statements	L3 (wk 1)	039–050	053–066	conditional-statements[184]
4	Valid and Invalid Arguments	L4 (wk 2)	051–063	066–079	valid-argument-forms[185]
5	Methods for Determining Validity	L5 (wk 2)	051–063	066–079	determining-argument-validity[186]
6	Quantified Statements	L5 (wk 2)	096–108	108–121	quantified-statements[187]
7	Negation of Quantified Statements	L6 (wk 2)	108–117	122–131	quantified-statements[188]
8	Statements with Multiple Quantifiers	L6 (wk 2)	117–131	131–146	quantified-statements[189]
9	Direct Proofs and Counterexamples	L7 (wk 3)	145–163	160–182	proof-techniques[190]
10	Proof by Contradiction	L8 (wk 3)	198–207	218–228	proof-techniques[191]
11	Proof by Contraposition	L9 (wk 3)	198–207	218–228	proof-techniques[192]
12	Rational Numbers	L9 (wk 3)	163–170	183–190	rational-and-irrational-numbers[193]
13	Divisibility	L10 (wk 4)	170–179	190–199	divisibility-and-factorisation[194]

[184] courses/math1061/conditional-statements.pdf
[185] courses/math1061/valid-argument-forms.pdf
[186] courses/math1061/determining-argument-validity.pdf
[187] courses/math1061/quantified-statements.pdf
[188] courses/math1061/quantified-statements.pdf
[189] courses/math1061/quantified-statements.pdf
[190] courses/math1061/proof-techniques.pdf
[191] courses/math1061/proof-techniques.pdf
[192] courses/math1061/proof-techniques.pdf
[193] courses/math1061/rational-and-irrational-numbers.pdf
[194] courses/math1061/divisibility-and-factorisation.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
14	Modular Arithmetic	L11 (wk 4)	482–485	528–531	modular-arithmetic[195]
15	The Euclidean Algorithm	L12 (wk 4)	220–224	250–254	gcd-lcm-and-euclidean-algorithm[196]
16	Sequences	L13 (wk 5)	227–244	258–275	sequences-and-summations[197]
17	Mathematical Induction	L13 (wk 5)	244–268	275–301	mathematical-induction[198]
18	Strong Induction and the Well Ordering Principle	L14 (wk 5)	268–279	301–314	strong-induction-and-the-well-ordering-principle[199]
19	Recursive Definitions	L15 (wk 6)	290–304	325–340	recursive-definitions[200]
20	Solving Recurrence Relations	L16 (wk 6)	304–328	340–364	solving-recurrence-relations[201]
21	Set Theory Definitions	L17 (wk 6)	336–351	377–391	sets-and-set-notation[202]
22	More Definitions and Examples of Sets	L17 (wk 6)	336–351	377–391	sets-and-set-notation[203]
23	Properties of Sets	L18 (wk 7)	352–366	391–407	proving-set-properties[204]

[195] courses/math1061/modular-arithmetic.pdf
[196] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[197] courses/math1061/sequences-and-summations.pdf
[198] courses/math1061/mathematical-induction.pdf
[199] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[200] courses/math1061/recursive-definitions.pdf
[201] courses/math1061/solving-recurrence-relations.pdf
[202] courses/math1061/sets-and-set-notation.pdf
[203] courses/math1061/sets-and-set-notation.pdf
[204] courses/math1061/proving-set-properties.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
24	Functions Defined on General Sets	L18 (wk 7)	383–396	425–439	functions-on-general-sets[205]
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	
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	

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

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
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[206].

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?

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

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

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[207].

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.

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 $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$.

[207] courses/math1061/logical-equivalence-laws.pdf

(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[208].

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.

[208] courses/math1061/conditional-statements.pdf

(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.

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	$q \vee r$	$p \rightarrow (q \vee r)$	$\sim q$	$p \wedge \sim q$	$(p \wedge \sim q) \rightarrow r$
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	$(p \rightarrow (q \vee r)) \leftrightarrow ((p \wedge \sim q) \rightarrow r)$
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 $(p \rightarrow (q \vee r)) \leftrightarrow ((p \wedge \sim q) \rightarrow r)$:

p	q	r	$p \rightarrow$	$(q \vee r)$	$\leftrightarrow$	$(p \wedge \sim q)$	$\rightarrow r$
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[209].

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.

[209] courses/math1061/valid-argument-forms.pdf

(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. $(p \wedge q) \rightarrow \sim r$
2. $p \vee \sim q$
3. $\sim q \rightarrow p \therefore \sim r$

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 ($p \rightarrow q$) 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[210].

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.

[210] courses/math1061/determining-argument-validity.pdf

(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

3. Give truth values for the variables p, q, r, s and w which demonstrate that the following argument is invalid.

$$[(p \vee q) \wedge (q \to r) \wedge ((p \wedge s) \to w) \wedge (\sim r) \wedge (q \to s)] \to w$$

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.	$(m \to n) \wedge (n \to m)$	from 1 by definition of $\leftrightarrow$
9.	$m \to n$	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. $r \to a$
2. $a \to s$
3. $s \to r$
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[211].

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

Problems

1. Rewrite each of the following in the form "$\forall$__, __." 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 "$\exists$__ 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) $\forall m, n \in \mathbb{Z}^+,\ mn \geq m + n$.

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) $\forall x \in \mathbb{R},\ (x \text{ is irrational} \rightarrow x \notin \mathbb{Z})$.

   (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[212].

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.

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 $xy \notin \mathbb{Z}$.

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

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[213].

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:

   (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.

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

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[214].

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*

   (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.

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

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

$$\begin{aligned} 4a + 2b &= 2\ell \quad \text{[Error: this line assumes what is to be proved.]} \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

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	$p \vee q$	$\sim p \vee r$	$(p \vee q) \wedge (\sim p \vee r)$	$q \vee r$	$\big((p \vee q) \wedge (\sim p \vee r)\big) \rightarrow (q \vee r)$
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[215].

Problems

1. Prove the following statement using a proof by contradiction:

$$\text{For integers } a \text{ and } b, \text{ if } 6a + 3b \text{ is odd, then } b \text{ is odd.}$$

2. Use a proof by contradiction to prove the following statement:

$$\text{For all positive integers } x \text{ and } y, \ x^2 - y^2 \neq 1.$$

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. □

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. □

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

§11 — Proof by Contraposition

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 9 (week 3). Notes: proof-techniques[216].

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.

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.

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

($\Leftarrow$) 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[217]*.*

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

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.

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. $\square$

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[218].

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:

   For all integers c, d and e, if $c \mid d$ and $c \nmid e$, 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.

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

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[219].

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 $58 \bmod 11$.

   (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 $r^2 \bmod 5$:

   $$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 4, \quad 4^2 \equiv 16 \equiv 1 \pmod 5.$$

   Thus $y^2 \equiv 0, 1$, or $4 \pmod 5$, and never 2 or 3. □

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

2. (a) Since $58 = 11 \cdot 5 + 3$ with $0 \le 3 < 11$, we have

$$58 \operatorname{div} 11 = 5 \quad \text{and} \quad 58 \bmod 11 = 3.$$

(b) We want $-95 = 11q + r$ with $0 \le r < 11$. 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[220].

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 $\operatorname{lcm}(116, 88)$.

[220] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

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

$$(y-1)(y^2-2)(y^3-3)(y^4-4) = \prod_{k=1}^{4} (y^k - k)\,.$$

(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 $n \geq 7$, $3^n < n!$. $\square$

(d) **For each integer $n \geq 1$, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.**

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 $n \geq 1$. $\square$

(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** $a_1, a_2, a_3, ...$ 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 $P(1), ..., P(k)$ 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 $P(0), P(1), ..., P(k)$ 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[221] — assessment weights and the full lecture schedule
- Logic: logical-connectives[222] · logical-equivalence-laws[223] · conditional-statements[224] · valid-argument-forms[225] · determining-argument-validity[226] · quantified-statements[227]
- Number theory and proof: proof-techniques[228] · rational-and-irrational-numbers[229] · divisibility-and-factorisation[230] · modular-arithmetic[231] · gcd-lcm-and-euclidean-algorithm[232]
- Graph theory (§43–§46): graphs[233] · walks-trails-and-circuits[234] · euler-circuits-and-trails[235] · adjacency-matrices[236] · incidence-matrices[237] · trees[238]

Subgroups and Cyclic Groups

A **subgroup** is a group sitting inside another group under the same operation. The quickest way to build one is to take a single element and all of its **powers**, positive, zero and negative: that set is the **cyclic subgroup** the element generates. A group that is the cyclic subgroup of one of its own elements is a **cyclic group**. The definition of a group is in [groups], and most of the examples live in integers-modulo-n[239]. First met in 2026-10-06-elementary-properties-of-groups[240], and cyclic groups are also worked in 2026-10-08-definitions-and-examples-of-fields[241].

[221] courses/math1061/math1061.pdf
[222] courses/math1061/logical-connectives.pdf
[223] courses/math1061/logical-equivalence-laws.pdf
[224] courses/math1061/conditional-statements.pdf
[225] courses/math1061/valid-argument-forms.pdf
[226] courses/math1061/determining-argument-validity.pdf
[227] courses/math1061/quantified-statements.pdf
[228] courses/math1061/proof-techniques.pdf
[229] courses/math1061/rational-and-irrational-numbers.pdf
[230] courses/math1061/divisibility-and-factorisation.pdf
[231] courses/math1061/modular-arithmetic.pdf
[232] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[233] courses/math1061/graphs.pdf
[234] courses/math1061/walks-trails-and-circuits.pdf
[235] courses/math1061/euler-circuits-and-trails.pdf
[236] courses/math1061/adjacency-matrices.pdf
[237] courses/math1061/incidence-matrices.pdf
[238] courses/math1061/trees.pdf
[239] courses/math1061/integers-modulo-n.pdf
[240] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[241] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf

Subgroups

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

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

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

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

Points to watch:

- **The same operation.** $\mathbb{R} - \{0\}$ is a group under multiplication, but it is not a subgroup of $(\mathbb{R}, +)$: under $+$ it is not closed, since $1 + (-1) = 0$, and it has no identity (2026-10-06-elementary-properties-of-groups[242]).
- **The identity of H is the identity of G.** If some $f \in H$ worked as an identity for H, then $f * f = f = f * e$ in G, and cancelling f on the left (groups[243]) gives $f = e$. So the identity check is simply: **is $e \in H$?** It also makes sure H is not empty.
- **The inverse of h in H is its inverse in G**, for the same reason: inverses in a group are unique (groups[244]). So the inverses check is: **for each $h \in H$, is $h^{-1} \in H$?**

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

[242] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[243] courses/math1061/groups.pdf
[244] courses/math1061/groups.pdf

H	G	Subgroup?	Why

H	G	Subgroup?	Why
$\mathbb{Z}$	$(\mathbb{R}, +)$	**yes**	$a + b \in \mathbb{Z}$, $0 \in \mathbb{Z}$, $-a \in \mathbb{Z}$ (2026-10-06-elementary-properties-of-groups[245])
$\mathbb{R} - \{0\}$	$(\mathbb{R}, +)$	**no**	$1 + (-1) = 0 \notin H$, and 0, the identity, is missing
$\{3n : n \in \mathbb{Z}\}$	$(\mathbb{Z}, +)$	**yes**	$3a + 3b = 3(a + b)$, $0 = 3 \cdot 0$, $-3a = 3(-a)$
$\{[0], [2], [4]\}$	$(\mathbb{Z}_6, +)$	**yes**	its block of the table uses only its own elements (cayley-tables[246])
$\{[0], [1]\}$	$(\mathbb{Z}_6, +)$	**no**	$[1] + [1] = [2] \notin H$

The multiples of 3 are Q1 of practice-problems[247], worked there in full.

Powers of an element

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

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

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

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

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

[245] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[246] courses/math1061/cayley-tables.pdf
[247] courses/math1061/practice-problems.pdf

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

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

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

The power laws

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

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

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

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

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

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

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

Worked: one negative power, three ways

$[3]^{-4}$ in $(\mathbb{Z}_7-\{[0]\},\cdot)$, where $[3]^4 = [81] = [4]$ (2026-10-06-elementary-properties-of-groups[248]):

- **Invert, then power.** $[3]^{-1} = [5]$, because $[3]\cdot[5] = [15] = [1]$. So $[3]^{-4} = [5]^4 = [25]\cdot[25] = [4]\cdot[4] = [2]$.

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

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

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

When the powers repeat

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

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

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

So in a finite group

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

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

The cyclic subgroup generated by a

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

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

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

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

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

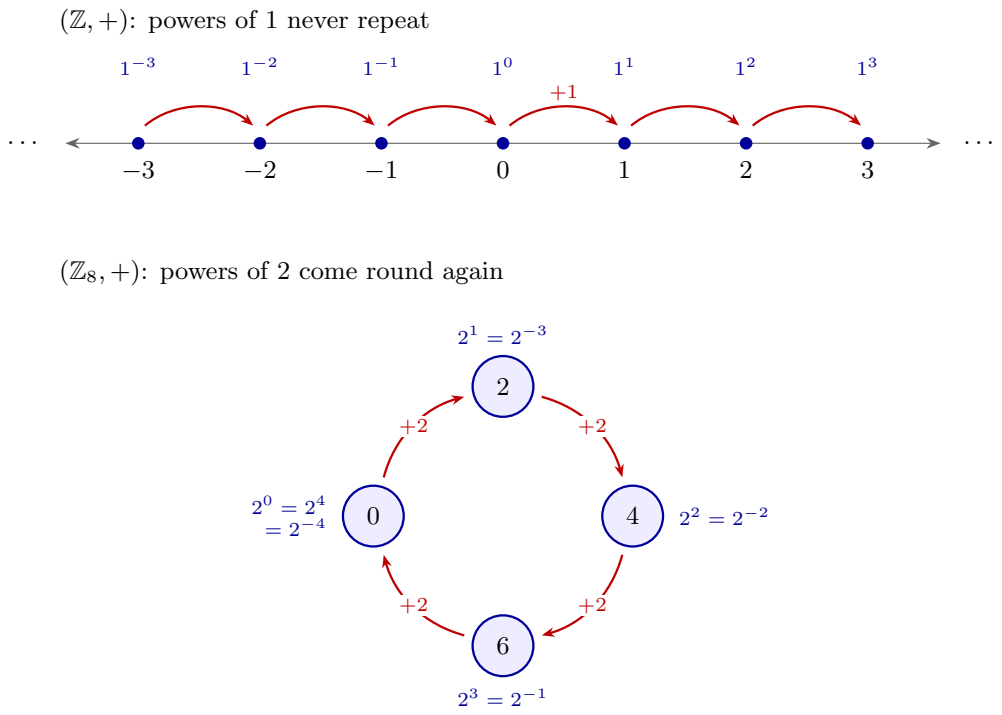


Figure 19: Powers of an element as steps, each step combining with the element once more; going left or backwards combines with its inverse. Top: in $(\mathbb{Z}, +)$ the powers of 1 run off in both directions and never repeat, so $\langle 1 \rangle$ needs the negative powers to reach $-1, -2, \ldots$. Bottom: in $(\mathbb{Z}_8, +)$ the powers of 2 come back to the identity at $2^4 = 0$, so the line closes into a loop of four. Every negative power lands on a positive one, such as $2^{-1} = 6 = 2^3$, and $\langle 2 \rangle = 2, 4, 6, 0$ is just the positive powers up to the identity.

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

Two rules that save work:

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

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

Worked examples

$\langle 3 \rangle$ **in** $(\mathbb{Z}_{11} - \{[0]\}, \cdot)$**.** The powers are $3, 9, 27 = 5, 15 = 4, 12 = 1$, so $\langle 3 \rangle = \{1, 3, 4, 5, 9\}$, five of the ten elements. Worked and drawn in 2026-10-06-elementary-properties-of-groups[249].

All the cyclic subgroups of $(\mathbb{Z}_8, +)$ (2026-10-06-elementary-properties-of-groups[250]):

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

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

All the cyclic subgroups of $(\mathbb{Z}_6, +)$**.** By the same method, $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$, $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$ and $\langle 3 \rangle = \{3, 0\}$. The subgroup $\langle 2 \rangle = \{0, 2, 4\}$ is the block in the table at 2026-10-06-elementary-properties-of-groups[251].

[249] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[250] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[251] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf

Cyclic groups

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

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

- **To prove G is cyclic**, name a generator a and show every element of G is a power of it. In a finite group, list the powers of a until the identity appears and count: if there are $|G|$ different ones, $\langle a \rangle = G$.
- **To prove G is not cyclic**, show that $\langle a \rangle \neq G$ for *every* $a \in G$. One element that fails to generate proves nothing.

Group	Cyclic?	Generators found	Where
$(\mathbb{Z}_{10}, +)$	yes	1	2026-10-06-elementary-properties-of-groups[252]
$(\mathbb{Z}_8, +)$	yes	$1, 3, 5, 7$	2026-10-06-elementary-properties-of-groups[253]
$(\mathbb{Z}_6, +)$	yes	$1, 5$	above
$(\mathbb{Z}_5 - \{[0]\}, \cdot)$	yes	$2, 3$	2026-10-06-elementary-properties-of-groups[254]
$(\mathbb{Z}_{11} - \{[0]\}, \cdot)$	yes	2, but not 3	practice-problems[255], Q4
$(\mathbb{Z}, +)$	yes	$1, -1$	2026-10-06-elementary-properties-of-groups[256]
$(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$	yes	$(1,1)$, $(1,2)$	below
$(\mathbb{Q}, +)$	**no**	none	below
$(S_3, \circ)$	**no**	none	symmetric-group[257]

[252] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[253] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[254] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[255] courses/math1061/practice-problems.pdf
[256] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[257] courses/math1061/symmetric-group.pdf

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

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

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

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

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

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

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

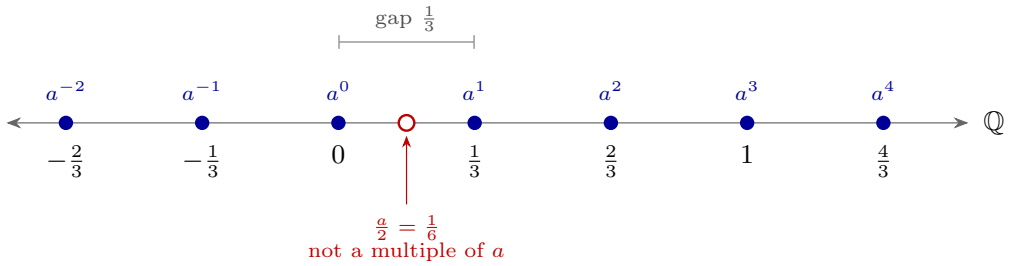


Figure 20: Why no rational number generates $(\mathbb{Q}, +)$, drawn for $a = \frac{1}{3}$. The powers of a under addition are its integer multiples, evenly spaced points a distance $\frac{1}{3}$ apart running off in both directions. Half of a, here $\frac{1}{6}$, is a rational number that falls in the gap between $a^0 = 0$ and $a^1 = \frac{1}{3}$, so it is not a power of a. Any other non-zero a has gaps of the same kind, and $a = 0$ generates only 0.

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

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

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

six different elements, so $\langle (1, 1) \rangle$ is the whole group and it is cyclic (2026-10-06-elementary-properties-of-groups[258]). Each step adds 1 to both coordinates. The first coordinate is back at

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

0 after every 2 steps, the second after every 3, and both are back together for the first time after 6, so the powers visit all six pairs before returning to $(0,0)$. Elements that move only one coordinate generate smaller subgroups:

$\langle(1,1)\rangle$: all 6

$(0,0)$ 6	$(0,1)$ 4	$(0,2)$ 2
$(1,0)$ 3	$(1,1)$ 1	$(1,2)$ 5

$\langle(0,1)\rangle$: 3 elements

$(0,0)$ 3	$(0,1)$ 1	$(0,2)$ 2
$(1,0)$	$(1,1)$	$(1,2)$

$\langle(1,0)\rangle$: 2 elements

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

Figure 21: Three cyclic subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_3$, each shaded inside the six-element group. A shaded cell is a power of the generator, and the small number in its corner is the k at which the generator's kth power first lands there. Left: $(1,1)$ changes both coordinates at every step and reaches all six pairs before $(1,1)^6 = (0,0)$, so it generates the whole group and the group is cyclic. Middle: $(0,1)$ never changes the first coordinate, so its powers stay in the top row and $\langle(0,1)\rangle$ has three elements. Right: $(1,0)$ never changes the second coordinate, so $\langle(1,0)\rangle = (0,0),(1,0)$.

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

Common mistakes

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

See also

- [groups] — the four properties, and the elementary properties such as the unique identity and $(g * h)^{-1} = h^{-1} * g^{-1}$
- cayley-tables[259] — a subgroup as a block of the table, when its elements are listed first
- integers-modulo-n[260] — $\mathbb{Z}_n$ and $\mathbb{Z}_n - \{[0]\}$, where most of the cyclic examples live
- symmetric-group[261] — the cyclic subgroups of S_3, a group that is not cyclic
- 2026-10-06-elementary-properties-of-groups[262] — Lecture 27 · 2026-10-08-definitions-and-examples-of-fields[263] — Lecture 28
- practice-problems[264] — §34, with full worked solutions

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[265] and composition-of-functions[266]. First met in 2026-09-24-definitions-and-examples-of-groups[267].

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[268]).

[259] courses/math1061/cayley-tables.pdf
[260] courses/math1061/integers-modulo-n.pdf
[261] courses/math1061/symmetric-group.pdf
[262] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[263] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[264] courses/math1061/practice-problems.pdf
[265] courses/math1061/one-to-one-and-onto-functions.pdf
[266] courses/math1061/composition-of-functions.pdf
[267] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[268] 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[269]). 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[270]). 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

[269] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[270] 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 $f_3 \circ f_2 = f_5$.

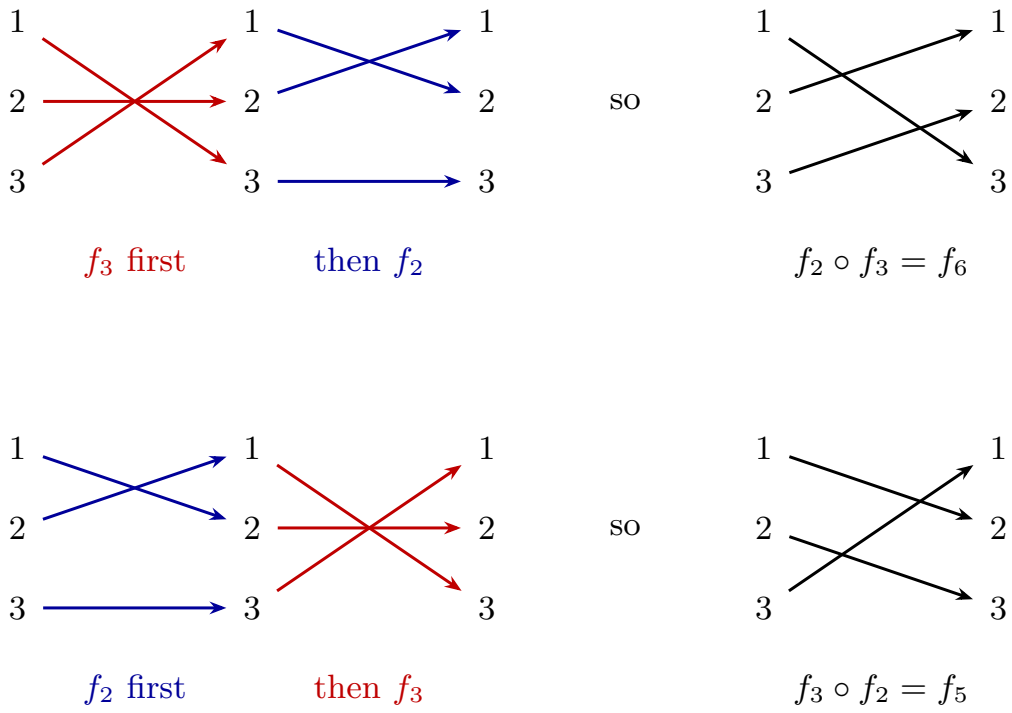


Figure 22: The same two elements of S_3 composed in both orders. Top: f_3 first and then f_2, which is $f_2 \circ f_3$. Following each number through both steps gives $1 \to 3$, $2 \to 1$, $3 \to 2$, the element f_6. Bottom: f_2 first and then f_3, which is $f_3 \circ f_2$. Now the result is $1 \to 2$, $2 \to 3$, $3 \to 1$, 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[271]). Each one also follows, for every n, from facts about functions:

- **Closure.** The composition of two bijections is a bijection (composition-of-functions[272]).
- **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[273]), which is again a bijection, and composing the two in either order gives the identity (composition-of-functions[274]).

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**.

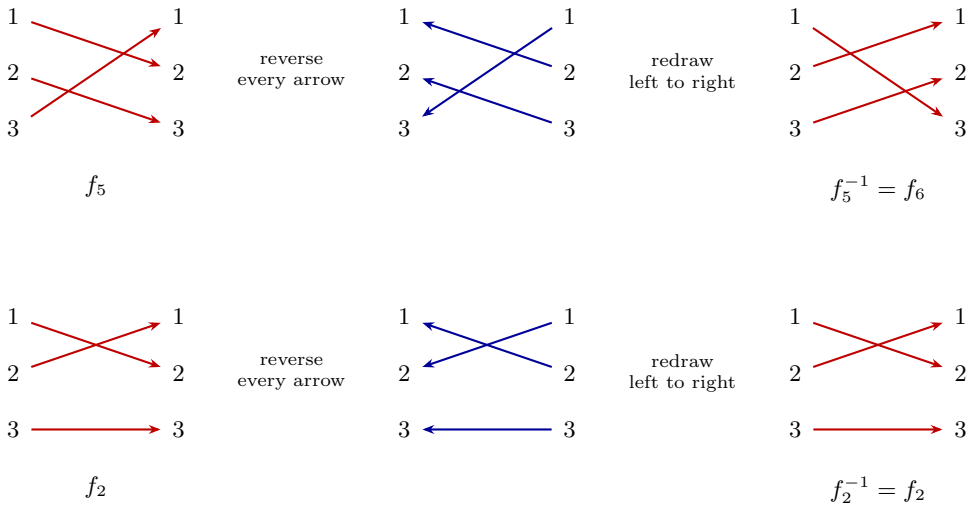


Figure 23: Inverses in S_3 by reversing arrows. Top: f_5 sends $1 \to 2$, $2 \to 3$, $3 \to 1$. Turning each arrow round gives $2 \to 1$, $3 \to 2$, $1 \to 3$, and reading that as a function of 1, 2, 3 gives $1 \to 3$, $2 \to 1$, $3 \to 2$, which is f_6. So $f_5^{-1} = f_6$. Bottom: f_2 swaps 1 and 2. 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.

[271] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[272] courses/math1061/composition-of-functions.pdf
[273] courses/math1061/inverse-functions.pdf
[274] 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[275]).

$\circ$	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[276]). 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.** $\langle f_1 \rangle = \{f_1\}$.

[275] courses/math1061/cayley-tables.pdf
[276] 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	$\{f_1, f_5, f_6\}$

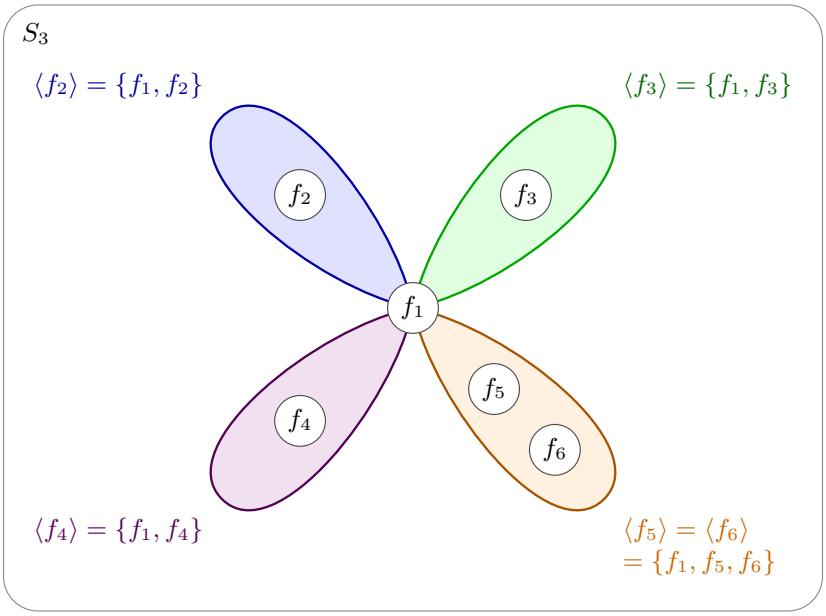


Figure 24: The cyclic subgroups of S_3, drawn inside it. Each petal is the set of powers of one element. The identity f_1, where the petals meet, is in every one, and it is the only element any two of them share. The three swaps f_2, f_3, f_4 each generate a subgroup of two elements, because a swap done 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[277]). $\{f_1, f_5, f_6\}$ also shows up as a block of the table when its elements are listed first (cayley-tables[278]).

[277] courses/math1061/subgroups-and-cyclic-groups.pdf
[278] 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[279] — reading a table, and why its rows and columns have no repeats
- composition-of-functions[280] — the operation of S_n, and why it is done right to left
- one-to-one-and-onto-functions[281] · inverse-functions[282] — bijections and their inverses, the elements of S_n and their group inverses
- functions-on-general-sets[283] — a function as a set of pairs
- subgroups-and-cyclic-groups[284] — powers, cyclic subgroups, and why a non-abelian group cannot be cyclic
- 2026-09-24-definitions-and-examples-of-groups[285] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[286] — Lecture 27
- practice-problems[287] — §33, with full worked solutions

[279] courses/math1061/cayley-tables.pdf
[280] courses/math1061/composition-of-functions.pdf
[281] courses/math1061/one-to-one-and-onto-functions.pdf
[282] courses/math1061/inverse-functions.pdf
[283] courses/math1061/functions-on-general-sets.pdf
[284] courses/math1061/subgroups-and-cyclic-groups.pdf
[285] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[286] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[287] courses/math1061/practice-problems.pdf