

1 Definitions and examples

Exercise 1.1. Determine which of the following sets are groups under the specified operations:

1. the integers under the operation of subtraction;
2. the set \mathbb{R} of real numbers under the operation \circ given by $a \circ b = a + b + 2$;
3. the set of odd integers under the operation of multiplication;
4. the set of $n \times n$ real matrices whose determinant is either 1 or -1 , under matrix multiplication.

Solution.

1. No, since no identity exists, because $x - e = x$ implies $e = 0$, but $0 - x = x$ does not hold for arbitrary x .

2. Yes, since:

(a) $a + b + 2 \in \mathbb{R}$

(b)

$$(a \circ b) \circ c = a \circ (b \circ c) \Leftrightarrow (a + b + 2) + c + 2 = a + (b + c + 2) + 2 \\ \Leftrightarrow a + b + c + 4 = a + b + c + 4$$

, which holds.

- (c) -2 is the identity element:

$$-2 \circ a = -2 + a + 2 = a = a \circ (-2)$$

- (d) $g^{-1} = -g - 4$:

$$g \circ g^{-1} = g - g - 4 + 2 = -2 = g^{-1} \circ g$$

3. No, since there is no multiplicative inverse in integers.

4. Yes, since:

- (a) A matrix product of $n \times n$ is an $n \times n$ matrix, and a determinant of such a product is a product of determinants of those matrices. Since the set $\{-1, 1\}$ is closed under multiplication, the set at hand is closed under matrix multiplication.

- (b) Matrix product is associative.

- (c) The identity matrix is the identity element and has $\det = 1$.

- (d) The inverse element is the matrix inverse. A^{-1} has determinant of ± 1 because $AA^{-1} = I$ and \det is distributive with respect to the matrix product:

$$AA^{-1} = I$$

$$\begin{aligned}
\det(AA^{-1}) &= \det I \\
\det A \cdot \det A^{-1} &= 1 \\
\pm 1 \cdot \det A^{-1} &= 1 \\
\det A^{-1} &= \mp 1
\end{aligned}$$

□

Exercise 1.2. Calculate the multiplication table for the following eight 2×2 complex matrices, and deduce that they form a non-abelian group:

$$\begin{aligned}
I &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \\
D &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad E = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad F = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad G = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}
\end{aligned}$$

Solution.

	I	A	B	C	D	E	F	G
I	I	A	B	C	D	E	F	G
A	A	B	C	I	E	F	G	D
B	B	C	I	A	F	G	D	E
C	C	I	A	B	G	D	E	F
D	D	G	F	E	I	C	B	A
E	E	D	G	F	A	I	C	B
F	F	E	D	G	B	A	I	C
G	G	F	E	D	C	B	A	I

Non-commutativity is trivial since $CD \neq DC$. Closure follows from the table, associativity is trivial, the identity element is I , and the inverse element can be found in the table for each element. □

Exercise 1.3. Find the multiplication table for the eight symmetries of a square.

Solution. None, since I can't automate it and I'm not calculating this by hand. □

Exercise 1.4. Find the symmetry groups of

1. a non-square rectangle,
2. a parallelogram with unequal sides which is not a rectangle,
3. a non-square rhombus.

Solution.

1. e , 180 degree rotations, reflection on both axis parallel to the rectangle's sides.
2. e , 180 degree rotations.
3. e , 180 degree rotations, reflection on both axis parallel to the rhombus's sides.

□

Exercise 1.5. Write down the multiplication tables for the groups $C_2 \times C_3$ and $C_3 \times C_3$.

Solution.

	(c_0, c_0)	(c_0, c_1)	(c_0, c_2)	(c_1, c_0)	(c_1, c_1)	(c_1, c_2)
(c_0, c_0)	(c_0, c_0)	(c_0, c_1)	(c_0, c_2)	(c_1, c_0)	(c_1, c_1)	(c_1, c_2)
(c_0, c_1)	(c_0, c_1)	(c_0, c_2)	(c_0, c_0)	(c_1, c_1)	(c_1, c_2)	(c_1, c_0)
(c_0, c_2)	(c_0, c_2)	(c_0, c_0)	(c_0, c_1)	(c_1, c_2)	(c_1, c_0)	(c_1, c_1)
(c_1, c_0)	(c_1, c_0)	(c_1, c_1)	(c_1, c_2)	(c_0, c_0)	(c_0, c_1)	(c_0, c_2)
(c_1, c_1)	(c_1, c_1)	(c_1, c_2)	(c_1, c_0)	(c_0, c_1)	(c_0, c_2)	(c_0, c_0)
(c_1, c_2)	(c_1, c_2)	(c_1, c_0)	(c_1, c_1)	(c_0, c_2)	(c_0, c_0)	(c_0, c_1)

Not doing the other one.

□

Exercise 1.6. Show that $G \times H$ is abelian if and only if G and H are each abelian.

Solution.

\Rightarrow Since $G \times H$ is abelian,

$$\begin{aligned}
 \forall i, j, k, l \quad (g_i, h_j)(g_k, h_l) &= (g_k, h_l)(g_i, h_j) \\
 (g_i g_k, h_j h_l) &= (g_i, h_j)(g_k, h_l) = (g_k, h_l)(g_i, h_j) = (g_k g_i, h_l h_j) \\
 (g_i g_k, h_j h_l) &= (g_k g_i, h_l h_j) \\
 g_i g_k &= g_k g_i \quad h_j h_l = h_l h_j
 \end{aligned}$$

\Leftarrow The same argument from the bottom up follows.

□

2 Maps and relations on sets

Exercise 2.1. Let $X = \{a, b, c\}$ and $Y = \{u, v\}$. List all the maps from X to Y and list all the maps from Y to X .

Solution. Maps from X to Y :

$$\begin{pmatrix} a & b & c \\ u & u & u \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ u & u & v \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ u & v & u \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ u & v & v \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ v & u & u \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ v & u & v \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ v & v & u \end{pmatrix} \quad \begin{pmatrix} a & b & c \\ v & v & v \end{pmatrix}$$

Maps from Y to X :

$$\begin{pmatrix} u & v \\ a & a \end{pmatrix} \quad \begin{pmatrix} u & v \\ a & b \end{pmatrix} \quad \begin{pmatrix} u & v \\ a & c \end{pmatrix} \quad \begin{pmatrix} u & v \\ b & a \end{pmatrix} \quad \begin{pmatrix} u & v \\ b & b \end{pmatrix} \quad \begin{pmatrix} u & v \\ b & c \end{pmatrix} \quad \begin{pmatrix} u & v \\ c & a \end{pmatrix} \quad \begin{pmatrix} u & v \\ c & b \end{pmatrix} \quad \begin{pmatrix} u & v \\ c & c \end{pmatrix}$$

□

Exercise 2.2. Let $g : X \rightarrow Y$ and $f : Y \rightarrow Z$ be functions. Show that:

1. if f and g are both injective then fg is injective;
2. if f and g are both surjective then fg is surjective.

Give examples to show that if f is injective and g is surjective then fg need neither be injective nor surjective.

Solution.

1. If $x_1 \neq x_2$ then $f(x_1) \neq f(x_2)$, therefore $g(f(x_1)) \neq g(f(x_2))$

- 2.

$$\forall z \in Z \quad \exists y \in Y : g(y) = z, \exists x \in X : f(x) = y \Rightarrow g(f(x)) = z$$

Let:

$$X = \{1, 2\}, \quad Y = \{3, 4, 5\}, \quad Z = \{6, 7\}, \quad f = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad g = \begin{pmatrix} 3 & 4 & 5 \\ 6 & 6 & 7 \end{pmatrix}$$

Then fg is:

$$fg = \begin{pmatrix} 1 & 2 \\ 6 & 6 \end{pmatrix}$$

, which is neither injective nor surjective.

□

Exercise 2.3. When $X = \{a, b, c\}$, list all the maps $f : X \rightarrow X$ which are constant (so that $f(a) = f(b) = f(c)$), Write down the composition table for these maps. Do these maps form a group?

Solution.

$$f = \begin{pmatrix} a & b & c \\ a & a & a \end{pmatrix} \quad g = \begin{pmatrix} a & b & c \\ b & b & b \end{pmatrix} \quad h = \begin{pmatrix} a & b & c \\ c & c & c \end{pmatrix}$$

	f	g	h
f	f	g	h
g	f	g	h
h	f	g	h

These maps do not form a group since no neutral element exists. □

Exercise 2.4. Prove that the relation on the set \mathbb{Z} defined by xRy if $x + y$ is an even integer is an equivalence relation, and determine the equivalence classes. Is the relation xRy if $x + y$ is divisible by 3 an equivalence relation?

Solution.

1. $xRy : x + y \equiv 0 \pmod{2}$ is an equivalence relation:

(a) xRx since $x + x = 2x \equiv 0 \pmod{2}$

(b) Symmetry follows from commutativity of addition.

(c) $xRy \Rightarrow y - x \equiv 0 \pmod{2}, yRz \Rightarrow z - y \equiv 0 \pmod{2} \Rightarrow z - x \equiv 0 \pmod{2} \Rightarrow z + x \equiv 0 \pmod{2} \Rightarrow zRx \Rightarrow xRz$

2. Equivalence classes:

$$[(x, y) : x \equiv y \pmod{2}] \quad [(x, y) : x \not\equiv y \pmod{2}]$$

3. No, because $1 + 1 \not\equiv 0 \pmod{3}$, therefore R is not reflective. □

Exercise 2.5. Write down the addition table for the congruence classes modulo 4, and the multiplication table for the non-zero congruence classes modulo 5.

Solution. Denoting congruence classes by smallest positive member of each class:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

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

□

Exercise 2.6. Show that multiplication of congruence classes modulo n is well-defined.

Solution. Need to prove that if $[x_1]_n = [x_2]_n$ and $[y_1]_n = [y_2]_n$ then $[x_1y_1]_n = [x_2y_2]_n$.

Let $x_1 = an + b, x_2 = cn + b, y_1 = en + d, y_2 = fn + d$

$$x_1y_1 = aen^2 + n(ab + be) + bd \equiv bd \pmod{n}$$

$$x_2y_2 \equiv bd \pmod{n}$$

Therefore x_1y_1 and x_2y_2 lie in the same congruence class.

□

3 Elementary consequences of the definitions

Exercise 3.1. Let G be a group in which $g^2 = 1$ for all g in G . Prove that G is abelian.

Solution. Proving from the bottom up:

$$\begin{aligned} xy &= yx \\ y &= x^{-1}yx \\ yx &= x^{-1}yx^2 \\ yx &= x^{-1}y \\ xy &= x^{-1}y \\ xy^2 &= x^{-1}y^2 \\ x &= x^{-1} \\ x^2 &= 1 \end{aligned}$$

, which holds.

□

Exercise 3.2. Let a, b and c be elements of the group G . Find the solutions x of the equations

1. $axa^{-1} = 1$,
2. $axa^{-1} = a$,
3. $axb = c$ and
4. $ba^{-1}xab^{-1} = ba$

Solution.

1.

$$\begin{aligned} axa^{-1} &= 1 \\ ax &= a \\ x &= a^{-1}a \\ x &= 1 \end{aligned}$$

2.

$$\begin{aligned} axa^{-1} &= a \\ ax &= a^2 \\ x &= a^{-1}a^2 \\ x &= a \end{aligned}$$

3.

$$\begin{aligned} axb &= c \\ ax &= cb^{-1} \\ x &= a^{-1}cb^{-1} \end{aligned}$$

4.

$$\begin{aligned} ba^{-1}xab^{-1} &= ba \\ ba^{-1}xa &= bab \\ ba^{-1}x &= baba^{-1} \\ a^{-1}x &= aba^{-1} \\ x &= a^2ba^{-1} \end{aligned}$$

□

Exercise 3.3. Let G be a group and c be a fixed element of G . Define a new operation $*$ on G by

$$x * y = xc^{-1}y$$

for all x and y in G . Prove that G is a group under the operation $*$.

Solution.

1. Closure is trivial.

2.

$$\begin{aligned} (x * y) * z &\stackrel{?}{=} x * (y * z) \\ (xc^{-1}y)c^{-1}z &\stackrel{?}{=} xc^{-1}(yc^{-1}z) \end{aligned}$$

, which holds by “extended associativity”, i.e. that brackets are meaningless.

3. The neutral element is c :

$$x * c = xc^{-1}c = x1 = x = 1x = cc^{-1}x = c * x$$

4. The inverse element is $cx^{-1}c$:

$$x * cx^{-1}c = xc^{-1}cx^{-1}c = x1x^{-1}c = xx^{-1}c = c$$

$$cx^{-1}c * x = cx^{-1}cc^{-1}x = c$$

□

Exercise 3.4. List the orders of all the elements of the group $D(3)$ of Example 1.9.

Solution.

Element	e	a	b	c	d	f
Order	1	2	2	1	1	1

□

Exercise 3.5. Give an example of a group G with elements x and y such that $(xy)^{-1}$ is not equal to $x^{-1}y^{-1}$.

Solution. $G = C_4, x = g, y = g^2$

$$xy = g^3 \quad (xy)^{-1} = g \quad x^{-1} = g^3 \quad y^{-1} = g^2 \quad x^{-1}y^{-1} = g^2 \neq (xy)^{-1}$$

□

Exercise 3.6. Let G be a group in which $(xy)^2 = x^2y^2$ for all x and y in G . Prove that G is abelian.

Solution.

$$\begin{aligned} xy &\stackrel{?}{=} yx \\ xxyy &\stackrel{?}{=} xyxy \\ x^2y^2 &= (xy)^2 \end{aligned}$$

, which holds by the definition of G . □

Exercise 3.7. Let x and g be elements of a group G . Prove, using mathematical induction, that for all positive integers k ,

$$(x^{-1}gx)^k = x^{-1}g^kx$$

Deduce that g and $x^{-1}gx$ have the same order.

Solution.

Base. $k = 0$.

$$(x^{-1}gx)^k = 1 = x^{-1}x = x^{-1}g^0x$$

Induction step.

$$(x^{-1}gx)^k = x^{-1}gx(x^{-1}gx)^{k-1} = x^{-1}gxx^{-1}g^{k-1}x = x^{-1}g^kx$$

Order:

\Rightarrow

$$g^k = 1 \Rightarrow x^{-1}g^kx = 1 \Rightarrow (x^{-1}gx)^k = 1$$

\Leftarrow

$$x^{-1}gx = 1 \Rightarrow x^{-1}g^kx = 1 \Rightarrow g^kx = x \Rightarrow g^k = 1$$

□

Exercise 3.8. Let ω denote the complex number $e^{2\pi i/6}$, so that $\omega^6 = 1$. Let

$$X = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$$

Show that $X^6 = I$ and calculate X^{-1} . Find a 2×2 matrix Y such that

$$XY = YX^{-1} \text{ and } Y^2 = X^3.$$

Show that the set $G = \{X^i, YX^j : 1 \leq i, j \leq 6\}$ with 12 elements is a group under matrix multiplication, and find the order of each element of G .

Solution.

$$X^6 = \begin{pmatrix} \omega^6 & 0 \\ 0 & \omega^{-6} \end{pmatrix} = I$$

$$X^{-1} = \begin{pmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{pmatrix}$$

Let $Y = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

$$Y^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix} = X^3 = \begin{pmatrix} \omega^3 & 0 \\ 0 & \omega^{-3} \end{pmatrix}$$

$$XY = \begin{pmatrix} a\omega & b\omega \\ c\omega^{-1} & d\omega^{-1} \end{pmatrix} \quad YX^{-1} = \begin{pmatrix} a\omega^{-1} & b\omega \\ c\omega^{-1} & d\omega \end{pmatrix}$$

This implies that $a = d = 0$. Therefore $bc = \omega^3 = -1$.

□