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)
   $$\begin{aligned}(a \circ b) \circ c = a \circ (b \circ c) &\Leftrightarrow (a + b + 2) + c + 2 = a + (b + c + 2) + 2 \\ &\Leftrightarrow a + b + c + 4 = a + b + c + 4\end{aligned}$$
   , 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:
   $$AA^{-1} = I$$

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

□

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

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

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.

$\square$

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. $\square$

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,

$$\forall i, j, k, l \quad (g_i, h_j)(g_k, h_l) = (g_k, h_l)(g_i, h_j)$$

$$(g_i g_k, h_j h_l) = (g_i, h_j)(g_k, h_l) = (g_k, h_l)(g_i, h_j) = (g_k g_i, h_l h_j)$$
$$(g_i g_k, h_j h_l) = (g_k g_i, h_l h_j)$$
$$g_i g_k = g_k g_i \quad h_j h_l = h_l h_j$$

$\Leftarrow$ The same argument from the bottom up follows.

$\square$

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 $g : X \to Y$ and $f : Y \to Z$ 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 $g(f(x_1)) \neq g(f(x_1))$
2. $$\forall z \in Z \;\; \exists y \in Y : g(y) = z, \exists x \in X : f(x) = y \Rightarrow g(f(x)) = z$$

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 $f : X \to X$ 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. $xRy : x + y \equiv 0 \mod 2$ is an equivalence relation:
   (a) xRx since $x + x = 2x \equiv 0 \mod 2$
   (b) Symmetry follows from commutativity of addition.
   (c) $xRy \Rightarrow y - x \equiv 0 \mod 2, yRz \Rightarrow z - y \equiv 0 \mod 2 \Rightarrow z - x \equiv 0 \mod 2 \Rightarrow z + x \equiv 0 \mod 2 \Rightarrow zRx \Rightarrow xRz$
2. Equivalence classes:

$$[(x, y) : x \equiv y \mod 2] \quad [(x, y) : x \not\equiv y \mod 2]$$

3. No, because $1 + 1 \not\equiv 0 \mod 3$, 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 $x_1 = an + b, x_2 = cn + b, y_1 = en + d, y_2 = fn + d$

$$x_1y_1 = aen^2 + n(ab + be) + bd \equiv bd \mod n$$

$$x_2y_2 \equiv bd \mod n$$

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. $$(x * y) * z \stackrel{?}{=} x * (y * z)$$
   $$(xc^{-1}y)c^{-1}z \stackrel{?}{=} xc^{-1}(yc^{-1}z)$$

   , 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.

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

, 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. $k = 0$.

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

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 $bc = \omega^3 = -1$. Let $c = -b^{-1}$.

The following is a proof of G being a group.

1. $\{X^i : 1 \leq i \leq 6\}$ is isomorphic to C_6 by a map that takes the first element of the first row and an inverse map $\omega^i \mapsto \begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{-i} \end{pmatrix}$. Closure of $\{X^i\}$ is therefore trivial. Moreover, $YX^j \times X^i = YX^{j+i \mod 6} \in G$. The following is the proof of two other cases.

$$\begin{aligned} X^i \times YX^j &= \begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{-i} \end{pmatrix} \times \left(\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix} \times \begin{pmatrix} \omega^j & 0 \\ 0 & \omega^{-j} \end{pmatrix} \right) \\ &= \begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{-i} \end{pmatrix} \times \begin{pmatrix} 0 & b\omega^{-j} \\ -b^{-1}\omega^j & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & b\omega^{i-j} \\ -b^{-1}\omega^{j-i} & 0 \end{pmatrix} \\ &= YX^{j-i \mod 6} \end{aligned}$$

$$\begin{aligned} YX^i \times YX^j &= \begin{pmatrix} 0 & b\omega^{-i} \\ -b^{-1}\omega^i & 0 \end{pmatrix} \times \begin{pmatrix} 0 & b\omega^{-j} \\ -b^{-1}\omega^j & 0 \end{pmatrix} \\ &= \begin{pmatrix} \omega^{j-i} & 0 \\ 0 & \omega^{i-j} \end{pmatrix} \\ &= X^{j-i \mod 6} \end{aligned}$$

2. Matrix product is associative.
3. The identity matrix is the identity element and is X^6.
4. The inverse for X^i is X^{6-i}, for YX^i is YX^{6-i}, which follows from the closure proof.

$\square$

4 Subgroups

Exercise 4.1. Which of the following sets H are subgroups of the given group G?

1. G is the set of integers under addition, H is the set of even integers;
2. $G = S(3), H = \{1, (12), (23), (13)\}$;
3. $G = GL(2, \mathbb{R}), H$ is the set of matrices of the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, where a is any real number.

Solution.

1. The identity element of $\mathbb{Z}_+$ is 0, which is contained in H. Moreover, even integers are closed under addition and the additive inverse of an integer is even. Therefore, all conditions of 4.2 (2) hold.
2. No, $(12)(23) \notin G$.
3. Let A_a denote $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. $A_a \times A_b = A_{a+b} \in H$, because reals are closed under addition. The identity element of G, I is A_0 and is therefore contained in H. The inverse of A_a is A_{-a}, which follows from the statements above.

□

Exercise 4.2. Give an example of a group G with subgroups H and K such that $H \cup K$ is not a subgroup of G.

Solution. Let G be an abelian group with distinct elements $1, k, h, hk$. Let $H = \langle h \rangle = \{1, h\}, K = \langle k \rangle = \{1, k\}$. $H \cup K$ does not contain hk, but contains h and k. □

Exercise 4.3. Let G be the group in Question 2 of Exercises 1. Find the number of elements in $\langle A, D \rangle$. Is $\langle A, C \rangle$ cyclic? Write down the multiplication table for $\langle B, F \rangle$.

Solution. $\langle A, D \rangle = \{I, A, D, B, E, G, C, F\}, |\langle A, D \rangle| = 8$

$\langle A, C \rangle = \{I, A, C, B\}$. This group is cyclic, which can be seen from its' Cayley table (see 1.2)

$\langle B, F \rangle = \{I, B, F, D\}$

	I	B	F	D
I	I	B	F	D
B	B	I	D	F
F	F	D	I	B
D	D	F	B	I

□

Exercise 4.4. Let G be the group with presentation $\{x, y : x^4 = 1, x^2 = y^2, xy = yx^{-1}\}$. Decide how many elements are in G and determine its multiplication table.

Solution. Consider the order of y. Since $y^4 = x^4 = 1$, it is ≤ 4.

If $y^3 = 1$, $x^2 y = 1$ and therefore $1 = xyx^{-1}$, which implies $y = 1, x^2 = 1$, which contradicts the definition of G.

If $y^2 = 1, x^2 = 1$, which contradicts the definition of G. From here onward, I will use the symbol "※" as a shorthand.

This proves $y^4 = 1$.

As per the argument given in the chapter, $xy^i = yx^i$ for all i.

Clearly, G contains all 3 powers of x and y. Let's consider xy.

Case 1: $xy = 1$
$y = x^{-1} = x^3, 1 = xy = yx^{-1} = x^3 x^{-1} = x^2$, ※

Case 2: $xy = x$
$y = 1, x = xy = yx^{-1} = x^{-1} \Rightarrow x^2 = 1$, ※

Case 3: $xy = x^2$
$y = x, x^2 = xy = yx^{-1} = yx^3 = x^4 = 1$, ※

Case 4: $xy = x^3$
$y = x^2 = y^2 \Rightarrow y = 1$, see case 2.

Case 5: $xy = y$
$x = 1$, ※

Case 6: $xy = y^3$
$x = y^2 = x^2 \Rightarrow x = 1$, ※

This proves that xy is in fact a distinct element of G. Let's consider xy^3 now.

Case 1: $xy^3 = 1$
$1 = xy^3 = yx \Rightarrow y = x^{-1} = x^3, 1 = xy^3 = xx^9 = x^2$, ※

Case 2: $xy^3 = x$
$y^3 = 1 \Rightarrow x^2 y = 1 \Rightarrow 1 = xyx^{-1} \Rightarrow y = 1 \Rightarrow x^2 = 1$, ※

Case 3: $xy^3 = x^2$
$x^3 y = x^2 \Rightarrow xy = x$, see case 2 for xy.

Case 4: $xy = x^3$
$y = x^2, y^2 = x^2 \Rightarrow y = 1$, see case 2 for xy

Case 5: $xy = y$
$x = 1$, ※

Case 6: $xy = y^3$
$x = y^2, x^2 = y^2 \Rightarrow x = 1$, ※

This proves that xy^3 is a distinct element of G. The following Cayley table proves closure:

	1	x	x^2	x^3	y	y^3	xy	xy^3
1	1	x	x^2	x^3	y	y^3	xy	xy^3
x	x	x^2	x^3	1	xy	xy^3	y^3	y
x^2	x^2	x^3	1	x	y^3	y	xy^3	xy
x^3	x^3	1	x	x^2	xy^3	xy	y	y^3
y	y	xy^3	xy	y	x^2	1	x^3	x
y^3	y^3	xy	y	xy^3	1	x^2	x	x^3
xy	xy	y	xy^3	y^3	x^3	x	x^2	1
xy^3	xy^3	y^3	xy	y	x	x^3	1	x^2

□

5 Cosets and Lagrange's Theorem

Exercise 5.1. Let G be the group of Question 2 in Exercises 1. Write down:

1. the list of left cosets of the subgroup $\langle A \rangle$ in G;
2. the list of left cosets of the subgroup $\langle B, F \rangle$ in G; and
3. the list of left cosets and the right cosets for the subgroup $\{I, D\}$.

Solution.

1. $\langle A \rangle = \{I, A, B, C\}$. The number of distinct left cosets of $\langle A \rangle$ is[1] $|G|/|\langle A \rangle| = 2$, so finding only two distinct left cosets suffices.

$$I \langle A \rangle = \langle A \rangle \quad D \langle A \rangle = \{I, D, G, F, E\}$$

2. $\langle B, F \rangle = \{I, B, F, D\}$, $|G|/|\langle B, F \rangle| = 2$.

$$I \langle B, F \rangle = \langle B, F \rangle \quad A \langle B, F \rangle = \{A, C, E, G\}$$

[1] By Lagrange's theorem.

3. $|G|/|\{I,D\}| = 4$. Left cosets:

$$I\{I,D\} = \{I,D\} \quad A\{I,D\} = \{A,E\} \quad B\{I,D\} = \{B,F\} \quad C\{I,D\} = \{C,G\}$$

Right cosets:

$$\{I,D\}I = \{I,D\} \quad \{I,D\}A = \{A,G\} \quad \{I,D\}B = \{B,F\} \quad \{I,D\}C = \{C,E\}$$

□

Exercise 5.2. Show that if the left coset gH is a subgroup of G, then g is in H.

Solution. All cosets are either equal or disjoint. Let us consider the two cosets gH and $1H$.

Case 1: $gH = 1H$
Then $\forall h \in H \;\; gh \in 1H = H$. Let $h = 1$, then $g1 = g \in H$

Case 2: $gH \cap 1H = \varnothing$
Since both gH and H are subgroups of the same group, they contain the same identity element, which contradicts the disjointness of gH and H.

□

Exercise 5.3. Show that if an element y of a group G is in the right coset Hx then $Hy = Hx$.

Solution.

$$y \in Hx \Rightarrow \exists \tilde{h} \in H : y = \tilde{h}x$$

We need to prove that $Hy = Hx$, that is $H\tilde{h}x = Hx$, which is trivial since $H\tilde{h} = H$ by closure of H. □

Exercise 5.4. Show that two right cosets Hx, Hy of a subgroup H in a group G are equal if and only if yx^{-1} is an element of H.

Solution.

- $\Rightarrow$

$$\forall h_1 \in H \;\; \exists h_2 \in H : h_1 y = h_2 x \Rightarrow h_1 y x^{-1} = h_2$$

  That is, $Hyx^{-1} = H$, which holds due to the previous exercise.

- $\Leftarrow$ $yx^{-1} \in H \Rightarrow H = Hyx^{-1}$ by closure of H.

□

Exercise 5.5. Give an example of a group G with subgroups A and B such that AB is not a subgroup of G.

Solution. $G = D(3)$ with the element names from chapter 1. $A = \langle d \rangle = \{e, d\}, B = \langle b \rangle = \{e, a, b\}. AB = \{e, d, f, c\}$, which is not a subgroup of G, since it doesn't contain $dc = b$. $\square$

Exercise 5.6. Let p be a prime number and G be a group with $p^a k$ elements, where a is a positive integer and p does not divide k. Suppose that P is a subgroup of G with p^a elements and Q is a subgroup of G with p^b elements, where $0 < b < a$. If Q is not a subgroup of P, show that PQ is not a subgroup of G.

Solution. Let $x = |P \cap Q|$. Since Q is a subgroup of P, $x > 0$ and $x < |Q| = p^b$ because $P \neq Q$. By proposition 5.18:

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{p^a p^b}{x} = \frac{p^{a+b}}{x}$$

Since $x < p^b$, x divides p at most p^{b-1} times and therefore $|PQ|$ divides p at least p^{a+1} times, therefore it does not divide $|G|$, which implies that PQ is not a subgroup of G. $\square$

6 Error-correcting codes

Exercise 6.1. For any element x in $\mathbb{Z}_2$, let $\overline{x}$ denote $1 + x$, so that $\overline{x}$ is 0 when x is 1 and $\overline{x}$ is 1 when x is zero. Let C be the set of elements of $V(6, 2)$ of the form $xyz\overline{xyz}$. Write down the eight elements of C, and show that C is not a linear code. What is the minimum distance of C?

Solution. The elements are $000111, 001110, 010101, 011100, 100011, 101010, 110001, 111000$.

C is not a linear code because it does not contain 000000, the neutral element of $V(6, 2)$.

The minimum distance of C cannot be 1 because if $y_1 \neq y_2$, then $\overline{y_1} \neq \overline{y_2}$ and

$$\rho(x_1 y_1 z_1 \overline{x_1 y_1 z_1}, x_2 y_2 z_2 \overline{x_2 y_2 z_2}) \geq 2$$

, same for x_1 and z_1. $\square$

Exercise 6.2. In each of the following cases, say how many errors the code with the given generator matrix G detects and how many errors the code corrects:

1. the code over $\mathbb{Z}_2$ with $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$
2. the code over $\mathbb{Z}_3$ with $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$
3. the code over $\mathbb{Z}_5$ with $G = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 4 & 1 \end{pmatrix}$

Solution.

1. All codewords are $\{00000, 00111, 01010, 10001, 001101, 10110, 11011, 11100\}$. The minimum weight of a codeword is 2, therefore the code detects one error and corrects none.
2. All codewords are $\{0000, 0112, 1011, 1120, 2022, 0221, 2101, 1202, 2210\}$. The minimum weight of a codeword is 3, therefore the code detects two errors and corrects one.
3. All codewords are of form $\begin{pmatrix} n & m & k & 2n+m+4k & n+3m+k \end{pmatrix}$. 21000 is such a codeword with weight of 3. Exhaustive shows it is the minimum weight, therefore the code detects two errors and corrects one.

□

Exercise 6.3. Let C be a linear code over $\mathbb{Z}_2$. Let C^+ be the subset of C consisting of those elements of C with even weight. Show that C^+ is an (additive) subgroup of C. By considering the cosets of the subgroup C^+ in C, show that either $C^+ = C$ or C^+ contains half the elements of C.

Solution.

1. C^+ is a subgroup:

   Closure is trivial by induction; the neutral element $0 \dots 0$ has weight 0, which is even and therefore the neutral element is in C^+; the additive inverse of x is x itself, and addition is clearly associative.

2. Consider xC^+.

   Case 1: $|x| \equiv 0 \mod 2$
   x is in C^+ and therefore xC^+ is C^+ by closure.

   Case 2: $|x| \equiv 1 \mod 2$
   x is not in C^+ and xC^+ contains precisely all elements of C with odd weight, since for any y of odd weight $y = x + z$, where $z = y - x$, which is of even weight and is therefore in C^+.

   If C has at least one element of odd weight, then the number of distinct left cosets is 2; 1 otherwise. Therefore $|C|/|C^+|$ is either 1 or 2, the claim follows.

□

Exercise 6.4. Construct a complete coset decoding table for the code in Question 2(b) above.

Solution.

0000	0112	1011	1120	2022	0221	2101	1202	2210
0001	0110	1012	1121	2020	0222	2102	1200	2211
0010	0122	1021	1100	2002	0201	2111	1212	2220
0100	0212	1111	1220	2022	0021	2201	1002	2010
1000	1112	2011	2120	2022	1221	0101	2202	0210
0011	0120	1022	1101	2000	0202	2112	1210	2221
1001	1110	2012	2121	2022	1222	0102	2200	0211
1010	1122	2021	2100	0002	1201	0111	1212	0220

□

Exercise 6.5. Calculate the parity check matrix for the code over $\mathbb{Z}_2$ with generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

and use it to construct the two-column decoding table. Decode the following:

1100011 1011000 0101110 0110001 1010110

Solution.

$$P = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

coset representative	syndrome
0000000	0000
0000001	0001
0000010	0010
0000100	0100
0001000	1000
0010000	1011
0100000	1110
1000000	1101
0000011	0011
0000101	0101
0000110	0110
0001001	1001
0001010	1010
0001100	1100
1000010	1111
0000111	0111

vector	syndrome	decoded
1100011	0000	1100011
1011000	1110	1111000
0101110	0000	0101110
0110001	0100	0110101
1010110	0000	1010110

□