A Book of Abstract Algebra - solutions to exercises

Otavio Macedo

December 23, 2020

Contents

Chapter 2

Set A

1. $a * b = \sqrt{|ab|}$ on the set $\mathbb{Q}$. This is not an operation on $\mathbb{Q}$. Square roots have two real solutions, some of them irrational. So, this operation is neither unique nor closed under $\mathbb{Q}$.

2. $a * b = a \ln b$, on the set $x \in \mathbb{R},\ x > 0$. This is not an operation because it's not closed. For instance, if $b = 1$ then $a \ln b = 0$, which does not belong to the set above.

3. $a * b$ is a root of the equation $x^2 - a^2b^2 = 0$, on the set $\mathbb{R}$. This is not an operation, since $a * b = \pm ab$, hence not unique.

4. Subtraction, on the set $\mathbb{Z}$. This is an operation.

5. Subtraction, on the set $n \in \mathbb{Z} : n \geq 0$. This is not an operation, since a subtraction of non-negative integers may result in a negative integer (not closed under the set).

Set B

1. $x * y = x + 2y + 4$. Commutative: no; Associative: no; Identity: no; Inverses: no.
   (i) $0 * 1 = 6$ and $1 * 0 = 5$.
   (ii) $x * (y * z) = x + 2y + 4z + 12$. $(x * y) * z = x + 2y + 2z + 4$.
   (iii) $x * e = x \Rightarrow x + 2e + 4 = x \Rightarrow 2e + 4 = 0 \Rightarrow e = -2$. But this value of e does not satisfy the equation $e * y = y$, since $-2 * y = -2 + 2y + 4 = 2y + 2 \neq y$.
   (iv) No identity implies no inverses.

2. $x * y = x + 2y - xy$. Commutative: no; Associative: no; Identity: no; Inverses: no.
   (i) $0 * 1 = 2$ and $1 * 0 = 1$.
   (ii) $(x * y) * z = 2y - xy - 2z - 2yz + xyz$ and $x * (y * z) = x + 2y + 4z - 2yz - xy - 2xz + xyz$.
   (iii) $x * e = x \Rightarrow x + 2e - xe = x \Rightarrow 2e - xe = 0 \Rightarrow e = 0$. But this value of e does not satisfy the equation $e * y = y$, since $0 * y = 2y \neq y$.
   (iv) No identity implies no inverses.

3. $x * y = |x + y|$. Commutative: yes; Associative: no; Identity: yes; Inverses: yes.
   (i) $|x + y| = |y + x|$.
   (ii) $||1 + -3| + -5| = 3$. But $|1 + | - 3 + -5|| = 9$.
   (iii) $x * e = x \Rightarrow |x + e| = x \Rightarrow e = 0$. Being commutative, $x * e = e * x$. So 0 is the identity.
   (iv) $x * x' = 0 \Rightarrow |x + x'| = 0 \Rightarrow x' = -x$. So, the inverse of x is $-x$.

4. $x * y = |x - y|$. Commutative: yes; Associative: no; Identity: yes; Inverses: yes.
   (i) $x - y = -(y - x) \Rightarrow |x - y| = | - (y - x)| = |y - x|$.

x	y	O_1	O_2	O_3	O_4	O_5	O_6	O_7	O_8	O_9	O_{10}	O_{11}	O_{12}	O_{13}	O_{14}	O_{15}	O_{16}
a	a	a	a	a	a	a	a	a	a	b	b	b	b	b	b	b	b
a	b	a	a	a	a	b	b	b	b	a	a	a	a	b	b	b	b
b	a	a	a	b	b	a	a	b	b	a	a	b	b	a	a	b	b
b	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b

Table 1: Operations on $\{a, b\}$

(ii) $||1-3|-5| = 3$. But $|1-|3-5|| = 1$.

(iii) $x * e = x \Rightarrow |x - e| = x \Rightarrow e = 0$. Being commutative, $x * e = e * x$. So 0 is the identity.

(iv) $x * x' = 0 \Rightarrow |x - x'| = 0 \Rightarrow x' = x$. So every element is its own inverse.

5. $x * y = xy + 1$. Commutative: yes; Associative: no; Identity: no; Inverses: no.

   (i) $xy + 1 = yx + 1$.

   (ii) $(x * y) * z = xyz + z + 1$. But $x * (y * z) = xyz + x + 1$.

   (iii) $x * e = x \Rightarrow xe + 1 = x$, which does not have a real solution.

   (iv) No identity implies no inverses.

6. $x * y = \max\{x, y\}$. Commutative: yes; Associative: yes; Identity: no; Inverses: no.

   (i) $\max\{x, y\} = \max\{y, x\}$.

   (ii) $\max\{x, \max\{y, z\}\} = \max\{\max\{x, y\}, z\}$.

   (iii) $x * e = x$ would imply that there exists an e that is smaller than any $x \in \mathbb{R}$, which is false.

   (iv) No identity implies no inverses.

Set C

Table 1 lists all the operations for the set $\{a, b\}$.

1. Commutative: $\{O_1, O_2, O_7, O_8, O_9, O_{10}, O_{15}, O_{16}\}$.

2. Associative: $\{O_1, O_2, O_4, O_6, O_7, O_8, O_{10}, O_{16}\}$.

3. Identity: $\{O_2, O_7, O_8, O_{10}\}$.

4. Inverses: $\{O_7, O_{10}\}$.

Set D

1. Let $a, b, c \in A^*$. Then:

$$(ab)c = (a_1 \dots a_m b_1 \dots b_n)c_1 \dots c_p = a_1 \dots a_m(b_1 \dots b_n c_1 \dots c_p) = a(bc)$$

2. Let $A = \{0, 1\}$ and $a = 001$ and $b = 110$, $a, b \in A^*$. Then $ab = 001110$ and $ba = 110001$, clearly showing that $ab \neq ba$.

3. Let $a\lambda = \lambda a = a$. So λ is the identity for this operation.

Chapter 3

Set A

1. $x * y = x + y + k$. Same thing as the example in Set B of Chapter 2, but with a generic constant k instead of the fixed constant 1.

2. $x * y = \frac{xy}{2}$, on the set $\{x \in \mathbb{R}, x \neq 0\}$.

   Commutative

$$\frac{xy}{2} = \frac{yx}{2}$$

Associative

$$(x*y)*z = \frac{xy}{2}*z = \frac{\frac{xy}{2}z}{2} = \frac{xyz}{4}$$
$$x*(y*z) = \frac{x(y*z)}{2} = \frac{x\frac{yz}{2}}{2} = \frac{xyz}{4}$$

Identity $x*e = x \Rightarrow \frac{xe}{2} = x \Rightarrow e = 2$

Inverse $x*x' = 2 \Rightarrow \frac{xx'}{2} = 2 \Rightarrow xx' = 4 \Rightarrow x' = \frac{4}{x}$

3. $x*y = x+y+xy$, on the set $\{x \in \mathbb{R}, x \neq -1\}$

   Commutative $x+y+xy = y+x+yx$

   Associative

$$(x*y)*z = (x+y+xy)*z = (x+y+xy)+x+(x+y+xy)z = x+y+z+xy+yz+xyz$$
$$x*(y*z) = x*(y+z+yz) = x+(y+z+yz)+x(y+z+yz) = x+y+z+xy+yz+xyz$$

   Identity $x*e = x \Rightarrow x+e+xe = x \Rightarrow x+e+xe-x = 0 \Rightarrow x(1+e-1)+e = 0 \Rightarrow xe+e = 0 \Rightarrow e = 0$

   Inverse $x*x' = 0 \Rightarrow x+x'+xx' = 0 \Rightarrow x = -x'(1+x) \Rightarrow x' = \frac{x}{1+x}$

4. $x*y = \frac{x+y}{xy+1}$, on the set $\{x \in \mathbb{R}, -1 < x < 1\}$.

   Commutative

$$\frac{x+y}{xy+1} = \frac{y+x}{yx+1}$$

   Associative

$$(x*y)*z = \frac{x+y}{xy+1}*z = \frac{\left(\frac{x+y}{xy+1}\right)+z}{\left(\frac{x+y}{xy+1}\right)z+1} = \frac{x+y+xyz+z}{xz+yz+xy+1}$$
$$x*(y*z) = x*\frac{y+z}{yz+1} = \frac{x+\left(\frac{y+z}{yz+1}\right)}{x\left(\frac{y+z}{yz+1}\right)+1} = \frac{x+y+xyz+z}{xz+yz+xy+1}$$

   Identity $e*x = x*e = x \Rightarrow \frac{x+e}{xe+1} = x \Rightarrow x+e = x(xe+1) \Rightarrow e = 0$

   Inverse $x'*x = x*x' = 0 \Rightarrow \frac{x+x'}{xx'+1} = 0 \Rightarrow x+x' = 0 \Rightarrow x' = -x$

Set B

1. $(a,b)*(c,d) = (ad+bc, bd)$, on the set $\{(x,y) \in \mathbb{R}\times\mathbb{R} : y \neq 0\}$: abelian group.

   Commutative: Yes $(ad+bc, bd) = (cb+da, bd)$

   Associative: Yes

$$[(a,b)*(c,d)]*(f,g) = (ad+bc, bd)*(f,g) = (adg+bcg+bdf, bdg)$$
$$(a,b)*[(c,d)*(f,g)] = (a,b)*(cg+df, dg) = (adg+bcg+bdf, bdg)$$

   Identity: Yes

$$\begin{aligned}(e_1,e_2)*(a,b) = (a,b)*(e_1,e_2) = (a,b) &\Rightarrow (ae_2+be_1, be_2) = (a,b)\\ &\Rightarrow \begin{cases} be_2 = b \Rightarrow e_2 = 1 \\ ae_2+be_1 = a \Rightarrow be_1 = 0 \Rightarrow e_1 = 0 \end{cases}\\ &\Rightarrow e = (0,1)\end{aligned}$$

   Inverse: Yes

$$\begin{aligned}(a',b')*(a,b) = (a,b)*(a',b') = (0,1) &\Rightarrow (ab'+ba', bb') = (0,1)\\ &\Rightarrow \begin{cases} bb' = 1 \Rightarrow b' = \frac{1}{b} \\ ab'+ba' = 0 \Rightarrow \frac{a}{b}+ba' = 0 \Rightarrow a' = -\frac{a}{b^2} \end{cases}\\ &\Rightarrow (a,b)' = \left(-\frac{a}{b^2}, \frac{1}{b}\right)\end{aligned}$$

2. $(a,b)*(c,d) = (ac, bc+d)$, on the set $\{(x,y) \in \mathbb{R}\times\mathbb{R} : x \neq 0\}$: non-abelian group.

   Commutative: No $(ac, bc+d) \neq (ca, da+b)$

   Associative: Yes

$$[(a,b)*(c,d)]*(f,g) = (ac, bc+d)*(f,g) = (acf, bcf+df+g)$$
$$[(a,b)*[(c,d)*(f,g)] = (a,b)*(cf, df+g) = (acf, bcf+df+g)$$

   Identity: Yes

$$\begin{aligned}(a,b)*(e_1,e_2) = (a,b) &\Rightarrow (ae_1+be_1, e_2) = (a,b)\\ &\Rightarrow \begin{cases} ae_1 = a \Rightarrow e_1 = 1 \\ be_1 + e2 = b \Rightarrow b + e_2 = b \Rightarrow e_2 = 0 \end{cases}\\ &\Rightarrow e = (1,0)\end{aligned}$$

   Not being commutative, we have to check the inverse order of the operands:

$$(1,0)*(a,b) = (1a+0a, b) = (a,b)$$

   Inverse: Yes

$$\begin{aligned}(a,b)*(a',b') = (1,0) &\Rightarrow (aa'+ba', b') = (1,0)\\ &\Rightarrow \begin{cases} aa' = 1 \Rightarrow a' = \frac{1}{a} \\ ba' + b' = 0 \Rightarrow \frac{b}{a} + b' = 0 \Rightarrow b' = -\frac{b}{a} \end{cases}\end{aligned}$$

   Not being commutative, we have to check the inverse order of the operands:

$$\left(\frac{1}{a}, -\frac{b}{a}\right)*(a,b) = \left(\frac{1}{a}a, -\frac{b}{a}a + b\right) = (1,0)$$

3. Same operation as in part 2, but on the set $\mathbb{R}\times\mathbb{R}$: not a group. There is no solution for the identity element.

4. $(a,b)*(c,d = (ac-bd, ad+bc)$, on the set $\mathbb{R}\times\mathbb{R}$, with the origin deleted: abelian group.

   Commutative: Yes $(ac-bd, ad+bc) = (ca-db, cb+da)$

   Associative: Yes

$$[(a,b)*(c,d)]*(f,g) = (ac-bd, ad+bc)*(f,g) = (acf-bdf-adg-bcg, acg-bdg+adf+bcf)$$
$$(a,b)*[(c,d)*(f,g)] = (a,b)*(cf-dg, cg+df) = (acf-adg-bcg-bdf, acg+adf+bcf-bdg)$$

   Identity: Yes

$$\begin{aligned}(e_1,e_2)*(a,b) = (a,b)*(e_1,e_2) = (a,b) &\Rightarrow (ae_1-be_2, ae_2+be_1) = (a,b)\\ &\Rightarrow \begin{cases} ae_1 - be_2 = a \Rightarrow e_1 = \frac{a+be_2}{a} \Rightarrow e_1 = 1 \\ be_2 + be_1 = b \Rightarrow ae_2 + b\left(\frac{a+be_2}{a}\right) = b \Rightarrow e_2 = 0 \end{cases}\\ &\Rightarrow e = (1,0)\end{aligned}$$

   Inverses: Yes

$$\begin{aligned}(a',b')*(a,b) = (a,b)*(a',b') = (1,0) &\Rightarrow (aa'-bb', ab'+ba') = (1,0)\\ &\Rightarrow \begin{cases} ab' + ba' = 0 \Rightarrow b' = -\frac{ba'}{a} \Rightarrow b' = -\frac{ba}{a^3+ab^2} \\ aa' - bb' = 1 \Rightarrow aa' + \frac{b^2a'}{a} = 1 \Rightarrow a' = \frac{a}{a^2+b^2} \end{cases}\\ &\Rightarrow (a,b)' = \left(\frac{a}{a^2+b^2}, -\frac{ba}{a^3+ab^2}\right)\end{aligned}$$

5. Consider the operation of the preceding problem on the set $\mathbb{R}\times\mathbb{R}$. Is this a group? Explain.
   This is not a group. The value for the identity is undefined.

$+$	$\varnothing$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	D
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	D
$\{a\}$	$\{a\}$	$\varnothing$	$\{a,b\}$	$\{a,c\}$	$\{b\}$	$\{c\}$	D	$\{b,c\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\varnothing$	$\{b,c\}$	$\{a\}$	D	$\{c\}$	$\{a,c\}$
$\{c\}$	$\{c\}$	$\{a,c\}$	$\{b,c\}$	$\varnothing$	D	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	D	$\varnothing$	$\{b,c\}$	$\{a,c\}$	$\{c\}$
$\{a,c\}$	$\{a,c\}$	$\{c\}$	D	$\{a\}$	$\{b,c\}$	$\varnothing$	$\{a,b\}$	$\{b\}$
$\{b,c\}$	$\{b,c\}$	D	$\{c\}$	$\{b\}$	$\{a,c\}$	$\{a,b\}$	$\varnothing$	$\{a\}$
D	D	$\{b,c\}$	$\{a,c\}$	$\{a,b\}$	$\{c\}$	$\{b\}$	$\{a\}$	$\varnothing$

Table 2: Operation table for $\langle P_D, +\rangle$

Set C

1. $e = \varnothing$, since $\varnothing + A = A + \varnothing = (A - \varnothing) \cup (\varnothing - A) = A \cup A = A$.
2. $A' + A = A + A' = \varnothing \Rightarrow (A - A') \cup (A' - A) = \varnothing \cup \varnothing = \varnothing$.
3. $P_D = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$. See table 2.

Set D

See Table 3 for the checkerboard game operation table. I is the identity since $X * I = I * X = X$ for any $X \in G$, and every element has an inverse (itself).

$*$	I	V	H	D
I	I	V	H	D
V	V	I	D	H
H	H	D	I	V
D	D	H	V	I

Table 3: Operation table for $\langle G, *\rangle$

Set E

See Table 4 for the coin game operation table. I is the identity, since $X * I = I * X = X$, for every $X \in G$. In every line there is an entry with I, which means that every element has an inverse. $\langle G, *\rangle$ is not commutative. For instance: $M_2 * M_4 \neq M_4 * M_2$.

$*$	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
I	I	M_1	M_2	M_3	M_4	M_5	M_6	M_7
M_1	M_1	I	M_3	M_2	M_5	M_4	M_7	M_6
M_2	M_2	M_3	I	M_1	M_6	M_7	M_4	M_5
M_3	M_3	M_2	M_1	I	M_7	M_6	M_5	M_4
M_4	M_4	M_6	M_5	M_7	I	M_2	M_1	M_3
M_5	M_5	M_7	M_4	M_6	M_1	M_3	I	M_2
M_6	M_6	M_4	M_7	M_5	M_2	I	M_3	M_1
M_7	M_7	M_5	M_6	M_4	M_3	M_1	M_2	I

Table 4: Operation table for $\langle G, *\rangle$

Set F

1.

$$\begin{aligned}(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) &= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)\\ &= (b_1 + a_1, b_2 + a_2, \ldots, b_n + a_n)\\ &= (b_1, b_2, \ldots, b_n) + (a_1, a_2, \ldots, a_n)\end{aligned}$$

2.

$$
\begin{aligned}
1+(0+1) &= 1+1=0=1+1=(1+0)+1\\
1+(0+0) &= 1+0=0=1+0=(1+0)+0\\
0+(1+1) &= 0+0=0=1+1=(0+1)+1\\
0+(0+1) &= 0+1=1=0+1=(0+0)+1\\
0+(1+0) &= 0+1=1=0+0=(0+1)+0\\
0+(0+0) &= 0+0=0=0+0=(0+0)+1
\end{aligned}
$$

3.

$$
\begin{aligned}
(a_1,\dots,a_n)+[(b_1,\dots,b_n)+(c_1,\dots,c_n)] &= (a_1,\dots,a_n)+(b_1+c_1,\dots,b_n+c_n)\\
&= (a_1+(b_1+c_1),\dots,a_n+(b_n+c_n))\\
&= ((a_1+b_1)+c_1,\dots,(a_n+b_n)+c_n)\\
&= [(a_1,\dots,a_n)+(b_1,\dots,b_n)]+(c_1,\dots,c_n)
\end{aligned}
$$

4. The identity is $(0,\dots,0)$, since $(a_1,\dots,a_n)+(0,\dots,0)=(a_1,\dots,a_n)=(0,\dots,0)+(a_1,\dots,a_n)$.
5. $(a_1,\dots,a_n)$ is its own inverse, since $(a_1,\dots,a_n)+(a_1,\dots,a_n)=(a_1+a_1,\dots,a_n+a_n)=(0,\dots,0)$.
6. $b=-b \Rightarrow a+b=a+(-b) \Rightarrow a+b=a-b$.
7. $a+b=c \Rightarrow a+b-b=c-b \Rightarrow a=c-b$. Since $-b=b$, $a=b+c$.

Set G

1. See Table 5.

	$a_4=a_1+a_3$	$a_5=a_1+a_2+a_3$
00000	$0=0+0$	$0=0+0+0$
00111	$1=0+1$	$1=0+0+1$
01001	$0=0+0$	$1=0+1+0$
01110	$1=0+1$	$0=0+1+1$
10011	$1=1+0$	$1=1+0+0$
10100	$0=1+1$	$0=1+0+1$
11010	$1=1+0$	$0=1+1+0$
11101	$0=1+1$	$1=1+1+1$

Table 5: Parity-check equations for C_1

2. $a_4=a_2$, $a_5=a_1+a_2$, $a_6=a_1+a_2+a_3$, $a_i\in\mathbb{B}$.
   (a) $C_2=\{000000, 001001, 010111, 011110, 100011, 101010, 110100, 111101\}$.
   (b) Minimum distance: 2 (e.g., 000000 and 001001).
   (c) There are $2^6=64$ words in $\mathbb{B}^6$ and there are 8 codewords in C_2. To be detected, a codeword must be transformed in a non-codeword. So there are $64-8=36$ ways of doing that.
3. $\{0000, 0101, 1011, 1110\}$, for equations $a_3=a_1$ and $a_4=a_1+a_2$. Minimum distance: 2.
4. Let dec be the decode function. So,

$$
\begin{aligned}
\text{dec}(11111) &= 11101\\
\text{dec}(00101) &= 00111\\
\text{dec}(11000) &= 11010\\
\text{dec}(10011) &= 10011\\
\text{dec}(10001) &= 10011\\
\text{dec}(10111) &= 10011, 00111
\end{aligned}
$$

5. If the minimum distance in a code is m, that means, by definition, that to transform one codeword into another, it is necessary to change at least m bits. Therefore, if less than m bits are changed, the result is a non-codeword and, as such, can be detected.

6. Let us assume that there is a certain element $x \in \mathbb{B} : x \in S_t(a) \cap S_t(b)$. Then the largest possible value of $d(a, b)$ is $2t = m - 1$. But it takes at least m errors to change one codeword into another. So, the premise is false and, therefore, $S_t(a) \cap S_t(b) \neq \varnothing$.

7. Let us say a codeword w is transformed into a non-codeword w' such that $d(w, w') \leqslant t$. Then $w' \in S_t(w)$. Since $S_t(w) \cap S_t(x) = \varnothing$ for any other codeword x, w' can be unambiguously decoded into w.

8. *I am probably wrong, but here is my reasoning, anyway*: the minimum distance in C_1 is 2. If that is the case, "two errors in any codeword can always be detected" is false. For instance, errors in positions 3 and 6 of 000000 result in 001001, another codeword, thus undetectable.

Chapter 4

Set A

1. $axb = c \Rightarrow aa^{-1}xb = a^{-1}c \Rightarrow xbb^{-1} = a^{-1}cb^{-1} \Rightarrow x = a^{-1}cb^{-1}$.

2. $x^2b = xa^{-1}c \Rightarrow x^{-1}xxb = x^{-1}xa^{-1}c \Rightarrow xb = a^{-1}c \Rightarrow xbb^{-1} = a^{-1}cb^{-1} \Rightarrow x = a^{-1}cb^{-1}$.

3. $x^2a = bxc^{-1} \Rightarrow x^2ac = bx$. But $xac = acx$, so $xacx = bx \Rightarrow xac = b \Rightarrow x = bc^{-1}a^{-1}$.

4. $ax^2 = b \Rightarrow ax^3 = bx$. But $x^3 = e$, so $x = b^{-1}a$.

5. $x^2 = a^2 \Rightarrow x^4 = a^4 \Rightarrow x^5 = a^4x$. But $x^5 = e$, so $e = a^4x \Rightarrow x = (a^4)^{-1}$.

6. $(xax)^3 = bx \Rightarrow xax^2ax^2ax = bx$. But $x^2a = a^{-1}x^{-1}$, so $xaa^{-1}x^{-1}a^{-1}x^{-1}x = bx \Rightarrow a^{-1} = bx \Rightarrow x = (ab^{-1})$.

Set B

1. False. $AA = I$, but $A \neq I$.

2. False. $AA = I = II$, but $A \neq I$.

3. False. $(AB)^2 = C^2 = I$, but $A^2B^2 = ID = D$.

4. True. $x^2 = x \Rightarrow xxx^{-1} = xx^{-1} \Rightarrow x = e$.

5. False. There is no y such that $y^2 = A$.

6. True. By the definition of groups, $x^{-1} \in G$. So $x^{-1}y = z \in G$ (groups are closed under the operation). Therefore $y = xz$.

Set C

1. $ab = ba \Rightarrow (ab)^{-1} = (ba)^{-1} \Rightarrow b^{-1}a^{-1} = a^{-1}b^{-1}$.

2. $a = b^{-1}ba \Rightarrow a = b^{-1}ab \Rightarrow ab^{-1} = b^{-1}a$.

3. $a(ab) = a(ba) = (ab)a$.

4. $a^2b^2 = aabb = abab = baba = bbaa = b^2a^2$.

5. $(xax^{-1})(xbx^{-1}) = xabx^{-1} = xbax^{-1} = (xbx^{-1})(xax^{-1})$.

6. (a) $aba^{-1} = b \Rightarrow aba^{-1}a = ba \Rightarrow ab = ba$
   (b) $ab = ba \Rightarrow aba^{-1} = baa^{-1} \Rightarrow aba^{-1} = b$

7. $e = ab(ab)^{-1} = ab(ba)^{-1} = aba^{-1}b^{-1}$.

Set D

1. $ab = e \Rightarrow a = b^{-1} = ba = bb^{-1} = e$.
2. $a(bc) = e \Rightarrow (bc)a = e$ (from item 1). Similarly, $(ab)c = e \Rightarrow cab = e$.
3. If $a_1 \dots a_n = e$, then the product of all a_i, in any order, is equal to e.
4. $xay = a^{-1} \Rightarrow xaya = e \Rightarrow yaxa = e \Rightarrow yax = e^{-1}$.
5. $ab = c \Rightarrow abc = e \Rightarrow bca = e \Rightarrow bc = a$. Also, $cab = e \Rightarrow ca = b$.
6. $abc = (abc)^{-1} \Rightarrow abcabc = e \Rightarrow bcabca = e \Rightarrow bca = (bca)^{-1}$. Also $cabcab = e \Rightarrow cab = (cab)^{-1}$.
7. $abba = aea = aa = e \Rightarrow ab = (ba)^{-1}$.
8. $a = a^{-1} \Rightarrow aa = a^{-1}a \Rightarrow aa = e$. Conversely, $aa = e \Rightarrow aaa^{-1} = ea^{-1} \Rightarrow a = a^{-1}$.
9. $ab = c \Rightarrow abc = cc = e$. Conversely, $abc = e \Rightarrow abcc = ec \Rightarrow ab = c$.

.

Set E

1. Let us use the Algorithm 1 to construct S.

Algorithm 1 Construction of S

procedure
    $S \leftarrow \varnothing$
    $G' \leftarrow$ copy of G
    while G' contains at least one element which is not its own inverse **do**
        Add to S one such element and its inverse
        Remove the pair from G'

First of all, note that at each step, the algorithm removes two elements from G'. Since G' is finite, the algorithm is guaranteed to terminate. At the end of each iteration, S gains two new elements. So the property that $|S|$ is even is guaranteed throughout. Finally, when the algorithm stops, G' does not contain any element that is its own inverse. Therefore, S is complete.

2. From item 1, we know that $|S| = 2k$, for some $k \in \mathbb{N}$. The number of elements that are equal to their own inverses is $|G| - |S|$. There are, then, two possiblities:

$$|G| - |S| = \begin{cases} 2(m-k) & \text{if } G = 2m\text{, for some } m \geqslant k \\ 2(m-k)+1 & \text{if } G = 2m+1\text{, for some } m \geqslant k \end{cases}$$

Thus if the number of elements in G is even, so is the number of elements in G that are equal to their own inverses. Likewise, if G has an ood number of elements.

3. If $|G|$ is even, $|G| - |S| = 2m$, for some $m \in \mathbb{N}$. But e is always its own inverse. So the number of elements $x \in G$ such that $x \neq e$ and $x = x^{-1}$ is $2n+1$, for some $0 \leqslant n < m$. So $2n + 1 \geqslant 1$.
4. Let $|S| = k$. Then $G = \{a_1, \dots, a_k, a_{k+1}, \dots, a_n\}$. G being abelian, we can rewrite $(a_1 \dots a_n)^2$ as

$$(a_1 \dots a_n)^2 = a_1 a_1^{-1} \dots a_k a_k^{-1} a_{k+1} a_{k+1}^{-1} \dots a_m a_m^{-1} = e$$

where $m = \frac{n-k}{2}$.

5. $a_1 \dots a_n = a_1 a_1^{-1} \dots a_{\frac{n}{2}} \; a_{\frac{n}{2}}^{-1} = e$.
6. Let's say, without loss of generality, that $a_1 \neq a_1^{-1}$. Then $a_1 \dots a_n = a_1 a_2 a_2^{-1} \dots a_{\frac{n-1}{2}} a_{\frac{n-1}{2}}^{-1} = a_1$.

Set F

1. (a) $a^2 = a \Rightarrow aaa^{-1} = aa^{-1} \Rightarrow a = e$.
   (b) $ab = a \Rightarrow a^{-1}ab = a^{-1}a \Rightarrow b = e$.
   (c) $ab = b \Rightarrow abb^{-1} = bb^{-1} \Rightarrow a = e$.
2. From exercise 4.B.6 we know that, for any two elements x and y in G there is an element z in G such that $y = xz$. In table terms, this means that in each row, every element appears at least once. Now let us assume that for certain x, y in G there are z_1, z_2 in G such that $y = xz_1 = xz_2$. Then $z_1 = z_2$. In table terms, this translates to each element in a row appearing in exactly one position.
3. See Table 6.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Table 6: Group with three elements

4. See Table 7.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 7: Group with four elements such that $xx = e$ for every $x \in G$

5. See Table 8.
6. **TODO**.

Set G

1. Prove that $G \times H$ is a group.

   (G1)
$$(x_1, y_1)[(x_2y_2)(x_3y_3)] = (x_1, y_1)(x_2x_3, y_2y_3) = (x_1x_2x_3, y_1y_2y_3)$$
$$[(x_1, y_1)(x_2y_2)](x_3y_3) = (x_1x_2, y_1y_2)(x_3, y_3) = (x_1x_2x_3, y_1y_2y_3)$$

   (G2) $e = (e_G, e_H)$, since $(x_1, y_1)(e_G, e_H) = (x_1, y_1) = (e_G, e_H)(x_1, y_1)$.
   (G3) $(x, y)^{-1} = (x^{-1}, y^{-1})$, since $(x, y)(x^{-1}, y^{-1}) = (e_G, e_H) = (x^{-1}, y^{-1})(x, y)$.
2. $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$. See Table 9 for the group operation.
3. $(g_1, h_1), (g_2, h_2) \in G \times H \Rightarrow (g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$. Since G and H are abelian, we can flip each multiplication in the tuple, resulting in $(g_2g_1, h_2h_1) = (g1, h_1)(g_2, h_2)$.
4. $(g, h)(g, h) = (gg, hh) = (e_G, e_H) = e_{G\times H}$.

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table 8: Group with four elements such that $xx = e$ for some $x \neq e \in G$ and $yy \neq e$ for some $y \in G$

Set H

1. For $n = 1$: $(bab^{-1}) = ba^{-1}b^{-1}$. Now suppose $(bab^{-1})^n = ba^nb^{-1}$ for some $n \geqslant 1$. Then:

$$(bab^{-1})^{n+1} = (bab^{-1})^n(bab^{-1}) = ba^nb^{-1}bab^{-1} = ba^nab^{-1} = ba^{n+1}b^{-1}$$

2. For $n = 1$: $(ab)^1 = a^1b^1$. Now suppose $(ab)^n = a^nb^n$, for some $n \geqslant 1$. Then:

$$(ab)^{n+1} = (ab)^n(ab) = a^nb^nab = a^nab^nb = a^{n+1}b^{n+1}$$

3. For $n = 1$: $(xa)^{2.1} = xaxa = ea = a = a^1$. Now suppose $(xa)^{2n} = a^n$ for some $n \geqslant 1$. Then:

$$(xa)^{2(n+1)} = (xa)^{2n+2} = (xa)^{2n}xaxa = a^nea = a^{n+1}$$

4. $a^3 = a^2 = e \Rightarrow a^{-1} = a^2 \Rightarrow (a^{-1})^2 = a^3a = a$. So $\sqrt{a} = a^{-1}$.
5. $a^2 = e \Rightarrow a^2a = ea \Rightarrow a^{-1} = a^2 \Rightarrow a^3 = a$. So $\sqrt[3]{a} = a$.
6. If there is some x such that $a^{-1} = x^3$, then $a = (a^{-1})^{-1} = (x^3)^{-1} = (xxx)^{-1} = x^{-1}x^{-1}x^{-1} = (x^{-1})^3$. Therefore, $\sqrt[3]{a} = x^{-1}$.
7.
8. $xax = b \Rightarrow axax = ab \Rightarrow (ax)^2 = ab \Rightarrow \sqrt{ab} = ax$.

Chapter 5

Set A

1. $G = \langle \mathbb{R}, +, \rangle$, $H = \{\log a : a \in \mathbb{Q}, a > 0\}$. H is a subgroup of G.
   (i) Suppose $\log a, \log b \in H$; then $\log a + \log b = \log(ab)$. Since $ab \in \mathbb{Q}$ and $ab > 0$, $\log(ab) \in H$. So H is closed under addition.
   (ii) Suppose $\log a \in H$; then $-\log a = \log a^{-1} = \log \frac{1}{a}$. Since $\frac{1}{a} \in \mathbb{Q}$ and $\frac{1}{a} > 0$, $-\log a \in H$.
2. $G = \langle \mathbb{R}, + \rangle$, $H = \{\log n : n \in \mathbb{Z}, n > 0\}$. H is *not* a subgroup of G.
   (i) Suppose $\log m, \log n \in H$; then $\log m + \log n = \log(mn)$. Since $mn \in \mathbb{Z}$ and $mn > 0$, $\log(mn) \in H$.
   (ii) Suppose $\log n \in H$; then $-\log n = \log \frac{1}{n}$. But $\frac{1}{n} \notin \mathbb{Z}$. So $-\log n \notin H$.
3. $G = \langle \mathbb{R}, + \rangle$, $H = \{x \in \mathbb{R} : \tan x \in \mathbb{Q}\}$. H is a subgroup of G.
   (i) Suppose $x, y \in H$; then $\tan(x + y) = \frac{\tan x + \tan y}{1 - \tan x \tan y}$, which is rational. So $x + y \in H$.
   (ii) Suppose $x \in H$; then $\tan(-x) = -\tan x \in \mathbb{Q}$. So $-x \in H$.
4. $G = \langle \mathbb{R}, \cdot \rangle$, $H = \{2^n3^m : m, n \in \mathbb{Z}\}$. H is a subgroup of G.
   (i) Suppose $2^n3^m, 2^p3^q \in H$; then $2^n3^m2^p3^q = 2^{n+p}3^{m+q}$. Since $n+p, m+q \in \mathbb{Z}$, H is closed under multiplication.
   (ii) Suppose $2^n3^m \in H$; then $(2^n3^m)^{-1} = 2^{-n}3^{-m}$. Since $-n, -m \in \mathbb{Z}$, H is closed under inverses.
5. $G = \langle \mathbb{R} \times \mathbb{R}, + \rangle$, $H = \{(x, y) : y = 2x\}$. H is a subgroup of G.

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

Table 9: Operation table for $\mathbb{Z}_2 \times \mathbb{Z}_3$

(i) Suppose $(x_1, 2x_1), (x_2, 2x_2) \in H$; then $(x_1, 2x_1) + (x_2, 2x_2) = (x_1 + x_2, 2(x_1 + x_2))$. So, H is closed under addition.
(ii) Suppose $(x, 2x) \in H$; then $-(x, 2x) = (-x, -2x) = (-x, 2(-x))$. So, H is closed under inverses.

6. $G = \langle \mathbb{R} \times \mathbb{R}, + \rangle$, $H = \{(x, y) : x^2 + y^2 > 0\}$. H is *not* a subgroup of G.

   (i) Suppose $(x, y) \in H$; then $(-x, -y)$ is also in H. But $(x, y) + (-x, -y) = (0, 0) \notin H$, since $0^2 + 0^2 = 0$. So, H is not closed under addition.

7. **TODO**.

Set B

1. $G = \langle \mathscr{F}(\mathbb{R}), + \rangle$, $H = \{f \in \mathscr{F}(\mathbb{R}) : f(x) = 0, \text{for every } x \in [0, 1]\}$. H is a subgroup of G.

   (i) Suppose $f, g \in H$; then, for every $x \in [0, 1]$, $[f + g](x) = f(x) + g(x) = 0 + 0 = 0$. So, $f + g \in H$.
   (ii) Suppose $f \in H$; then, for every $x \in [0, 1]$, $[-f](x) = -f(x) = 0$. So, $-f \in H$.

2. $G = \langle \mathscr{F}(\mathbb{R}), + \rangle$, $H = \{f \in \mathscr{F}(\mathbb{R}) : f(-x) = -f(x)\}$. H is a subgroup of G.

   (i) Suppose $f, g \in H$; then $[f + g](-x) = f(-x) + g(-x) = -f(x) - g(x) = -(f(x) + g(x) = -[f + g](x)$. So, $f + g \in H$.
   (ii) Suppose $f \in H$; then $[-f](-x) = -f(-x) = -(-f(x)) = f(x)$. So, $-f \in H$.

3. $G = \langle \mathscr{F}(\mathbb{R}), + \rangle$, $H = \{f \in \mathscr{F}(\mathbb{R}) : f \text{ is periodic of period } \pi\}$. H is a subgroup of G.

   (i) Suppose $f, g \in H$; then $[f + g](x + n\pi) = f(x + n\pi) + g(x + n\pi) = f(x) + g(x) = [f + g](x)$. So, $f + g \in H$.
   (ii) Suppose $f \in H$; then $[-f](-x) = -f(x + n\pi) = -f(x) = f(x)$. So, $-f \in H$.

4. $G = \langle \mathscr{C}(\mathbb{R}), + \rangle$, $H = \{f \in \mathscr{C}(\mathbb{R}) : \int_0^1 f(x)dx = 0\}$.

   (i) Suppose $f, g \in H$; then $\int_0^1 [f+g](x)dx = \int_0^1 [f(x)+g(x)]dx = \int_0^1 f(x)dx + \int_0^1 g(x)dx = 0+0 = 0$. So, $f+g \in H$.
   (ii) Suppose $f \in H$; then $\int_0^1 [-f](x)dx = -\int_0^1 f(x)dx = 0$. So $-f \in H$.

5. $G = \langle \mathscr{D}(\mathbb{R}), + \rangle$, $H = \{f \in \mathscr{D}(\mathbb{R}) : df/dx \text{ is constant}\}$.

   (i) Suppose $f, g \in H$; then $d[f + g]/dx = df/dx + dg/dx = k$, where k is a constant. So, $f + g \in H$.
   (ii) Suppose $f \in H$; then $d[-f]/dx = -df/dx$, which is also a consntant. So $-f \in H$.

6. $G = \langle \mathscr{F}(\mathbb{R}), + \rangle$, $H = \{f \in \mathscr{F}(\mathbb{R}) : f(x) \in \mathbb{Z} \text{ for every } x \in \mathbb{R}\}$.

   (i) Suppose $f, g \in H$; then $[f + g](x) = f(x) + g(x) \in \mathbb{Z}$. So, $f + g \in H$.
   (ii) Suppose $f \in H$; then $[-f](x) = -f(x) \in \mathbb{Z}$. So $-f \in H$.

Set C

1. Let $x, y \in H$; then $xy = x^{-1}y^{-1} = (yx)^{-1} = (xy)^{-1}$. So $xy \in H$. And, by the definition of H, $x^{-1} \in H$.

2. Let $x, y \in H$; then $(xy)^n = x^n y^n = ee = e$. So $xy \in H$. And $(x^{-1})^n = (x^n)^{-1} = e^{-1} = e$. So, $x^{-1} \in H$.

3. Let $x_1, x_2 \in H$; then $x_1 x_2 = y_1^2 y_2^2 = (y_1 y_2)^2$. So $x_1 x_2 \in H$. And $x_1^{-1} = (y_1^2)^{-1} = (y_1^{-1})^2$. So, $x_1^{-1} \in H$.

4. Let $x, y \in K$; then $(xy)^2 = x^2 y^2 \in H$. So $xy \in K$. And $(x^{-1})^2 = (x^2)^{-1} \in H$. So, $x^{-1} \in K$.

5. Let $x, y \in K$; then $x^m, y^n \in H$, for some integers m, n. By the definition of group, we can multiply any element of H by itself and the result will be in H. That is, $x^{km}, y^{kn} \in H$, for any integer $k > 0$. In particular, $x^{nm}, y^{mn} \in H$ and, thus, $x^{nm} y^{mn} = (xy)^{nm} \in H$. So, $x \in K$. And $(x^m)^{-1} = (x^{-1})^m \in H$. So, $x^{-1} \in K$.

6. Let $z_1, z_2 \in HK$; then there are $x_1, x_2 \in H$ and $y_1, y_2 \in K$ such that $z_1 z_2 = x_1 y_1 x_2 y_2 = x_1 x_2 y_1 y_2 \in HK$. And $z_1^{-1} = (x_1 y_1)^{-1} = x^{-1} y^{-1} \in HK$.

7. The proofs in parts 4-6 depend on being able to reorder the elements in a multiplication. If G is not abelian, this is not possible.

Set D

1. Let $x, y \in H \cap K$; then $xy \in H$ because both x and y are in H. Analogously, $xy \in K$. So $xy \in H \cap K$. And $x^{-1} \in H$ and $x^{-1} \in K$. So $x^{-1} \in H \cap K$.

2. Let $x, y \in H$. Since H is a group, $xy \in H$ and the operation is the same as in K. Similarly, $x^{-1} \in H$.

3. Let $a, b \in C$; then $abx = axb = xab$, for any $x \in G$. So $ab \in C$. And $(a^{-1}x)^{-1} = x^{-1}a = ax^{-1} = (xa^{-1})^{-1}$. So, $a^{-1}x = xa^{-1}$ and, thus, $a^{-1} \in C$.

4. Let $a, b \in C'$; then $(abx)^2 = abxabx = xabxab = (xab)^2$. So $ab \in C'$. And $((a^{-1}x)^2)^{-1} = (a^{-1}xa^{-1}x)^{-1} = x^{-1}ax^{-1}a = (x^{-1}a)^2 = ((a^{-1}x)^2)^{-1}$. So $a^{-1} \in C'$.

5. Let us consider the elements $a_ia_1, a_ia_2, \ldots, a_ia_n$ for some $a_i \in S$ and let us assume that $e \notin S$; then $a_ia_j \neq a_i$ for any $a_j \in S$. This observation, along with the fact that G is a finite group, allows us to conclude that $a_ia_1 \neq a_ia_2 \neq \ldots \neq a_ia_n \neq a_i$. S being closed, this would imply that S has $n+1$ elements, which is a contradiction and, therefore, $e \in S$.

   Now let us assume that there is some $a_i \in S$ such that $a_i^{-1} \notin S$; then $a_ia_j \neq e$ for any $a_j \in S$. Similar to the observation above, this would imply that S has $n+1$ elements (all a_ia_j plus e). Therefore S is closed under inverses.

6. Let P be the set of all periods of f and $a, b \in P$; then $f(abx) = f(bx) = f(x)$ for any $x \in G$. And $f(x) = f(aa^{-1}x) = f(a^{-1}x)$ for any $x \in G$. So P is closed under multiplication and inverses.

7. (a) Let $x, y \in K$ and $a \in H$; then $xya(xy)^{-1} = xyay^{-1}x^{-1} \in H$. Conversely, assuming $xya(xy)^{-1} \in H$ implies that $yay^{-1} \in H$, which implies that $a \in H$. So $xy \in K$. And $a \in H \Rightarrow xx^{-1}axx^{-1} \in H \Rightarrow x^{-1}ax \in H$. Conversely, assuming that $x^{-1}ax \in H$ implies that $xx^{-1}ax x^{-1} \in H \Rightarrow a \in H$. So $x^{-1} \in H$. Thus, K is closed under multiplication and inverses.

   (b) Let $a, b \in H$ and $x \in K$; then $xax^{-1} \in H$ and $xbx^{-1} \in H$. Since H is a group (see previous item), $xax^{-1}xb^{-1} = xabx^{-1} \in H$. The proof in the other direction is basically the same. And, since H is a group, $(xax^{-1})^{-1} = xa^{-1}x^{-1} \in H$ (similar proof in the other direction). So, H is closed under multiplication and inverses.

8. (a) Let $x_1, x_2 \in G$; then $(x_1, e)(x_2, e) = (x_1x_2, e) \in G \times H$. And $(x_1, e)^{-1} = (x_1^{-1}, e) \in G \times H$. So $G \times H$ is closed under multiplication and inverses.

   (b) Let $x_1, x_2 \in G$; then $(x_1, x_1)(x_2, x_2) = (x_1x_1, x_2x_2) \in G \times G$. And $(x_1, x_1)^{-1} = (x_1^{-1}, x_1^{-1}) \in G \times G$. So $G \times G$ is closed under multiplication and inverses.

Set E

1. $\langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 0\}$
   $\langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \{2, 4, 6, 8, 0\}$
   $\langle 5 \rangle = \{5, 0\}$
   $\langle 8 \rangle = \{8, 2, 0\}$
   $\langle 0 \rangle = \{0\}$

2. $0 = 5 + 5$
   $1 = 5 + 2 + 2 + 2$
   $2 = 2$
   $3 = 5 + 2 + 2 + 2 + 2$
   $4 = 2 + 2$
   $5 = 5$
   $6 = 2 + 2 + 2$
   $7 = 5 + 2$
   $8 = 2 + 2 + 2 + 2$
   $9 = 5 + 2 + 2$

3. $\langle 6, 9 \rangle$ is the subset of $\mathbb{Z}$ whose elements are multiples of 3 modulo 12, that is, $\{6, 9, 3, 0\}$.

4. $\langle 10, 15 \rangle$ is the subset of the integers that are multiples of 5.

5. Let's start with the following equality: $1 = 7.3 + 5.(-4)$. For any integer n, if we multiply by n on both sides, we get $n = 7(3n) + 5(-4n)$. In other words, any $n \in \mathbb{Z}$ can be written as a sum of a certain number of 7's plus a sum of another number of 5's. In the context of the additive group of the intergers, this means that $\mathbb{Z} = \langle 7, 5 \rangle$.

6. $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle$, since we can multiply $(1,1)$ by the integers from 1 to 5, obtaining $(1,1)$, $(0,2)$, $(1,0)$, $(0,1)$, $(1,2)$, $(0,0)$, respectively, which exhausts the whole set. Similarly, $\mathbb{Z}_3 \times \mathbb{Z}_4$ can be obtained by multiplying $(1,1)$ by the integers from 1 to 12. arg

7. Let us assume that there is an element $(1, y)$ that is the generator of $\mathbb{Z}_2 \times \mathbb{Z}_4$ (the first integer of the tuple cannot possibly be 0, otherwise it would be impossible to generate non-zero integers at the first position). To generate different elements, we have to multiply that generator by different integers, so all elements would be of the form $(n \mod 2, yn \mod 4)$, with $n \in \mathbb{Z}$. In particular, to generate $(0,1)$, the following system of equations must be satisfied:

$$\begin{aligned} n &\mod 2 = 0 \Rightarrow n = 2p, p \in \mathbb{Z} \\ yn &\mod 4 = 1 \Rightarrow ny = 4q + 1, q \in \mathbb{Z} \end{aligned}$$

which implies that $2py = 4q + 1$, which has no solution, contradicting our initial assumption. So, $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not cyclic.

On the other hand, any element of $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_4$ can be written as $(1n + 1m \mod 2, 1n + 2m \mod 4)$, as listed in Table 10.

n	m	x	y
0	0	0	0
3	3	0	1
2	2	0	2
1	1	0	3
2	1	1	0
1	2	1	1
4	1	1	2
7	0	1	3

Table 10: Multiples of the generators of $\mathbb{Z}_2 \times \mathbb{Z}_4$

8. If $ab = ba$ then $a^{-1}b^{-1} = b^{-1}a^{-1}$ and $ab^{-1} = b^{-1}a$ and $a^{-1}b = ba^{-1}$. Given any $x, y \in G$, xy can be written as a sequence of elements from $\{a, a^{-1}, b, b^{-1}\}$. yx can also be written as a sequence of the same elements, only possibly in a different order. But since all these elements commute, we can rearrange them (let's say $a^m b^n$, with $m, n \in \mathbb{Z}$) so that $xy = yx$.

Set F

1. See Table 11.

	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

Table 11: Operation table of G

2. See Table 12.

3. See Table 13.

4. See Table 14.

	e	a	b	b^2	b^3	ab	ab^2	ab^3
e	e	a	b	b^2	b^3	ab	ab^2	ab^3
a	a	e	ab	ab^2	ab^3	b	b^2	b^3
b	b	ab^3	b^2	b^3	e	a	ab	ab^2
b^2	b^2	ab^2	b^3	e	b	ab^3	a	ab
b^3	b^3	ab	e	b	b^2	ab^2	ab^3	a
ab	ab	b^3	ab^2	ab^3	a	e	b	b^2
ab^2	ab^2	b^2	ab^3	a	ab	b^3	e	b
ab^3	ab^3	b	a	ab	ab^2	b^2	b^3	e

Table 12: Operation table of the dihedral group D_4

	e	a	b	b^2	b^3	ab	ab^2	ab^3
e	e	a	b	b^2	b^3	ab	ab^2	ab^3
a	a	b^2	ab	ab^2	ab^3	b^3	e	b
b	b	ab^3	b^2	b^3	e	a	ab	ab^2
b^2	b^2	ab^2	b^3	e	b	ab^3	a	ab
b^3	b^3	ab	e	b	b^2	ab^2	ab^3	a
ab	ab	b	ab^2	ab^3	a	b^2	b^3	e
ab^2	ab^2	e	ab^3	a	ab	b	b^2	b^3
ab^3	ab^3	b^3	a	ab	ab^2	e	b	b^2

Table 13: Operation table for the quaternion group

Set G

1. See Table 15.
2. See Table 16.
3. See Table 17.
4. This is the dihedral group D_4. See Table 12.
5. See Table 18.
6. See Table 19.

Set H

1. $\mathbf{G}_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$, $\mathbf{H}_2 = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$.

2. $\mathbf{G}_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$, $\mathbf{H}_3 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$.

	e	a	b	c	ab	bc	ac	abc
e	e	a	b	c	ab	bc	ac	abc
a	a	e	ab	ac	b	abc	c	bc
b	b	ab	e	bc	a	c	abc	ac
c	c	ac	bc	e	abc	b	a	ab
ab	ab	b	a	abc	e	ac	bc	c
bc	bc	abc	c	b	ac	e	ab	a
ac	ac	c	abc	a	bc	ab	e	b
abc	abc	bc	ac	ab	c	a	b	e

Table 14: Operation table for the commutative group

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Table 15: Operation table for item 1

	e	a	b	ab	ba	aba
e	e	a	b	ab	ba	aba
a	a	e	ab	b	aba	ba
b	b	ba	e	aba	a	ab
ab	ab	aba	a	ba	e	b
ba	ba	b	aba	e	ab	a
aba	aba	ab	ba	a	b	e

Table 16: Table operation for item 2

	e	a	b	ab	ba	bab	aba	$abab$
e	e	a	b	ab	ba	bab	aba	$abab$
a	a	e	ab	b	aba	$abab$	ba	bab
b	b	ba	e	bab	$abab$	ab	$abab$	aba
ab	ab	aba	a	$abab$	e	b	bab	ba
ba	ba	b	bab	e	$ababa$	aba	a	ab
bab	bab	$abab$	ba	aba	b	e	ab	a
aba	aba	ab	$abab$	a	bab	ba	e	b
$abab$	$abab$	bab	aba	ba	ab	a	b	e

Table 17: Operation table for item 3

	e	a	b	b^2	b^3	ab	ab^2	ab^3
e	e	a	b	b^2	b^3	ab	ab^2	ab^3
a	a	e	ab	ab^2	ab^3	b	b^2	b^3
b	b	ab	b^2	b^3	e	ab^2	ab^3	a
b^2	b^2	ab^2	b^3	e	b	ab^3	a	ab
b^3	b^3	ab^3	e	b	b^2	a	ab	ab^2
ab	ab	b	ab^2	ab^3	a	b^2	b^3	e
ab^2	ab^2	b^2	ab^3	a	ab	b^3	e	b
ab^3	ab^3	b^3	a	ab	ab^2	e	b	b^2

Table 18: Operation table for item 5

.

	e	a	b	b^2	ab	ab^2	ba	bab	bab^2	b^2a	b^2ab	aba
e	e	a	b	b^2	ab	ab^2	ba	bab	bab^2	b^2a	b^2ab	aba
a	e	e	ab	ab^2	b	b^2	aba	b^2a	b^2ab	bab	bab^2	ba
b	b	ba	b^2	e	bab	bab^2	b^2a	b^2ab	aba	a	ab	ab^2
b^2	b^2	b^2a	e	b	b^2ab	aba	a	ab	ab^2	ba	bab	bab^2
ab	ab	aba	ab^2	a	b^2a	b^2ab	bab	bab^2	ba	e	b	b^2
ab^2	ab^2	bab	a	ab	bab^2	ba	e	b	b^2	aba	b^2a	b^2ab
ba	ba	b	bab	bab^2	b^2	e	ab^2	a	ab	b^2ab	aba	b^2a
bab	bab	ab^2	bab^2	ba	a	ab	b^2ab	aba	b^2a	b	b^2	e
bab^2	bab^2	b^2ab	ba	bab	aba	b^2a	b	b^2	e	ab^2	a	ab
b^2a	b^2a	b^2	b^2ab	aba	e	b	bab^2	ba	bab	ab	ab^2	a
b^2ab	b^2ab	bab^2	aba	b^2a	ba	bab	ab	ab^2	a	b^2	e	b
aba	aba	ab	b^2a	b^2ab	ab^2	a	b^2	e	b	bab^2	ba	bab

Table 19: Operation table for item 6

3. By the definition of the addition operation for this group, $\mathbf{x}+\mathbf{y}$ has 1 in the positions where $\mathbf{x}$ and $\mathbf{y}$ differ, and 0 in the positions where they equal. So, the number of 1s in $\mathbf{x}+\mathbf{y}$ is the same as the distance between $\mathbf{x}$ and $\mathbf{y}$.

4. From the previous item, $d(\mathbf{x},\mathbf{0}) = w(\mathbf{x}+\mathbf{0}) = w(\mathbf{x})$.

5. Let $\mathbf{x},\mathbf{y} \in C$ such that $d(\mathbf{x},\mathbf{y})$ is the minimum distance in C. Now let us assume that there is some $\mathbf{z} \in C$ such that $w(\mathbf{z}) < d(\mathbf{x},\mathbf{y})$. Now, $\mathbf{z}$ can be written as the sum of two other elements, say $\mathbf{z} = \mathbf{x}' + \mathbf{y}'$; then $w(\mathbf{z}) = w(\mathbf{x}'+\mathbf{y}') = d(\mathbf{x}',\mathbf{y}') < d(\mathbf{x},\mathbf{y})$, which is a contradiction, since $d(\mathbf{x},\mathbf{y})$ is the minimum distance. Therefore, the minimum distance in C is equal to the minimum weight in C, namely $w(\mathbf{x}+\mathbf{y})$.

6. For the items below, let p be the number of positions in which $\mathbf{x}$ and $\mathbf{y}$ are both 1 .
   (a) Let us say that $w(\mathbf{x}) = 2m$ and $w(\mathbf{y}) = 2n$. Then $w(\mathbf{x}+\mathbf{y}) = 2m + 2n - 2p = 2(m+n-p)$, which is even.
   (b) Let us say that $w(\mathbf{x}) = 2m+1$ and $w(\mathbf{y}) = 2n+1$. Then $w(\mathbf{x}+\mathbf{y}) = 2m+1+2n+1-2p = 2(m+n-p+1)$, which is even.
   (c) Let us say that $w(\mathbf{x}) = 2m+1$ and $w(\mathbf{y}) = 2n$. Then $w(\mathbf{x}+\mathbf{y}) = 2m+1+2n-2p = 2(m+n-p)+1$, which is odd.$13x_1 + 4 = 3x_2 + 4 \Rightarrow x_1 = x_2 13x_1 + 4 = 3x_2 + 4 \Rightarrow x_1 = x_2$. f is surjective: for every $y \in \mathbb{R}$, $f()$. f is surjective: for every $y \in \mathbb{R}$, $f()$

7. Let us say a group code C of order m has n elements with odd weight (and consequently $m-n$ elements with even weight), with $0 < n \leqslant m$. Then, let us take one of these elements with odd weight and multiply by each element of the group, obtaining the whole group: $\{xa_1, xa_2, \ldots, xa_m\}$, $a_i \in C$. In all the instances in which a_i has even weight, xa_i has odd weight. Since there are $m-n$ such instances, there are $m-n$ elements with odd weight, which means that $m-n=n$ and, therefore, $n = \frac{m}{2}$. In the case in which all elements have even weight, this property is trivially satisfied, since the weight of the product of any two elements with even weight is even.

8. $\mathbf{H}(\mathbf{x}+\mathbf{y}) = \mathbf{Hx} + \mathbf{Hy} = 0 \Leftrightarrow \mathbf{Hx} = \mathbf{Hy}$.

Chapter 6

Set A

1. f is bijective: $f^{-1}(x) = (x-4)/3$.
   Range: $\mathbb{R}$.

2. f is bijective: $f^{-1}(x) = \sqrt[3]{x-1}$.
   Range: $\mathbb{R}$.

3. f is not injective: $|x| = |-x| = x$ for any $x \in \mathbb{R}$. f is surjective: $|y| = y$, for any $y \in \mathbb{R}$.
   Range: $\{x \in \mathbb{R} : x \geqslant 0\}$.

4. f is not injective: $f(-1) = f(2) = 2$. f is surjective because it is continuous and unbounded.
   Range: $\mathbb{R}$.

5. f is bijective:

$$f^{-1}(x) = \begin{cases} x & \text{if } x \text{ is rational} \\ \frac{x}{2} & \text{if } x \text{ is irrational} \end{cases}$$

   Range: $\mathbb{R}$.

6. f is injective, but not surjective: for any odd number y, there is no x such that $f(x) = y$.
   Range: $\{x \in \mathbb{Z} : x = 2k, \text{for all } k \in \mathbb{Z}\} \cup \{x \notin \mathbb{Z}\}$.

Set B

1. f is bijective: $f^{-1}(x) = \ln(x)$.

2. f is bijective: $f^{-1}(x) = \arctan(x)$.

3. f is not injective: given $f(x_1) = f(x_2)$, x_1 and x_2 can independently be any number in $\{y :\in \mathbb{R} : x_i - 1 < y \leqslant x_i\}$. f is surjective: any integer maps to itself.

4. f is bijective: $f^{-1} = f$.

5. $f(n) = 2n$.

Set C

1. f is not injective: take $f(x, y_1) = f(x, y_2)$ even when $y_1 \neq y_2$. f is surjective: any element $x \in A$ is the image of (x, y), for any $y \in B$.

2. f is bijective: $f^{-1} = f$.

3. f is injective, but not surjective: none of the elements in the set $\{x \in B : x \neq b\}$ is an image of any element in A.

4. f is bijective: $f^{-1}(x) = a^{-1}x$.

5. f is bijective: $f^{-1} = f$.

6. f is not bijective: take, for example the group of Table 15; in that case, $a^2 = b^2 = e$. f is not surjective: take, for example $\langle \mathbb{Z}, + \rangle$; in this case $f(x) = 2x$, which means that odd numbers are not the image of any element in $\mathbb{Z}$.

Set D

1. $(f \circ g)(x) = \sin(e^x)$; $(g \circ f)(x) = e^{\sin(x)}$.
   $f \circ g : \mathbb{R} \to \mathbb{R}$; $g \circ f : \mathbb{R} \to \mathbb{R}$.

2. $(g \circ f)(x, y) = y$.
   $g \circ f : A \times B \to B$.

3. $(g \circ f)(x) = \ln(1/x)$; $f \circ g$ would be defined as $(f \circ g)(x) = 1/\ln x$, but $(f \circ g)(1) = 1/0$, which is undefined.
   $g \circ f : (0, 1) \to \mathbb{R}$.

4. $f \circ g = g \circ f$, which consists of spelling every word backwards and interchanging the letters a with o, i with u and e with y.
   $g \circ f$: Latin alphabet $\to$ Latin alphabet.

5. $f \circ g = \begin{bmatrix} a & b & c & d \\ c & a & c & a \end{bmatrix}$, $g \circ f = \begin{bmatrix} a & b & c & d \\ b & b & b & b \end{bmatrix}$.
   $g \circ f : \{a, b, c, d\} \to \{a, b, c, d\}$.

6. $(f \circ g)(x) = abx$; $(f \circ g)(x) = bax$;
   $f \circ g : G \to G$; $g \circ f : G \to G$.

Set E

1. $f^{-1} = f$.

2. $f^{-1}(x) = \ln x$.

3. $f^{-1}(x) = \sqrt[3]{x - 1}$.

4. $f^{-1}(x) = \begin{cases} x/2 & \text{if } x \text{ is rational} \\ x/3 & \text{if } x \text{ is irrational} \end{cases}$

5. $f^{-1} = \begin{bmatrix} 3 & 1 & 2 & 4 \\ a & b & c & d \end{bmatrix}$

6. $f^{-1}(x) = a^{-1}x$