# A Book of Abstract Algebra - solutions to exercises

Otavio Macedo

January 22, 2021

## Contents

**Chapter 2** **3**
Set A . . . 3
Set B . . . 3
Set C . . . 4
Set D . . . 4

**Chapter 3** **4**
Set A . . . 4
Set B . . . 5
Set C . . . 6
Set D . . . 6
Set E . . . 7
Set F . . . 7
Set G . . . 8

**Chapter 4** **8**
Set A . . . 8
Set B . . . 9
Set C . . . 9
Set D . . . 9
Set E . . . 9
Set F . . . 10
Set G . . . 11
Set H . . . 11

**Chapter 5** **12**
Set A . . . 12
Set B . . . 12
Set C . . . 13
Set D . . . 13
Set E . . . 14
Set F . . . 15
Set G . . . 15
Set H . . . 17

**Chapter 6** **17**
Set A . . . 17
Set B . . . 18
Set C . . . 18
Set D . . . 18
Set E . . . 19
Set F . . . 19
Set G . . . 19
Set H . . . 19
Set I . . . 21

**Chapter 7** **24**
Set A . . . 24
Set B . . . 24
Set C . . . 24
Set D . . . 25
Set E . . . 25
Set F . . . 25
Set G . . . 25
Set H . . . 25
Set I . . . 26

**Chapter 8** **26**
Set A . . . 26
Set B . . . 27
Set C . . . 28
Set D . . . 29
Set E . . . 29
Set F . . . 29
Set G . . . 30
Set H . . . 30

**Chapter 9** **30**
Set A . . . 30
Set B . . . 31
Set C . . . 31
Set D . . . 31
Set E . . . 31
Set F . . . 32
Set G . . . 32
Set H . . . 33
Set I . . . 33

**Chapter 10** **33**
Set A . . . 33
Set B . . . 34
Set C . . . 35
Set D . . . 35
Set E . . . 36
Set F . . . 36
Set G . . . 37
Set H . . . 37

**Chapter 11** **37**
Set A . . . 37
Set B . . . 38
Set C . . . 38
Set D . . . 38
Set E . . . 39

**Chapter 15** **39**
Set G . . . 39
Set H . . . 40

**Chapter 16** **40**
Set L . . . 40
Set M . . . 40

# 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) $x - y = -(y - x) \Rightarrow |x - y| = |-(y - x)| = |y - x|$.
   (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.

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

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

### 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 $\lambda$ 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**

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

   **Inverse: Yes**

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

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**

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

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

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

**Inverse: Yes**

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

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**

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

   **Inverses: Yes**

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

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.

## 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 $\langle G, * \rangle$

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

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

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

4. The identity is $(0, \ldots, 0)$, since $(a_1, \ldots, a_n) + (0, \ldots, 0) = (a_1, \ldots, a_n) = (0, \ldots, 0) + (a_1, \ldots, a_n)$.

5. $(a_1, \ldots, a_n)$ is its own inverse, since $(a_1, \ldots, a_n) + (a_1, \ldots, a_n) = (a_1 + a_1, \ldots, a_n + a_n) = (0, \ldots, 0)$.

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,
$$\text{dec}(11111) = 11101$$
$$\text{dec}(00101) = 00111$$
$$\text{dec}(11000) = 11010$$
$$\text{dec}(10011) = 10011$$
$$\text{dec}(10001) = 10011$$
$$\text{dec}(10111) = 10011, 00111$$
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 $S$

```
1: procedure
2:     S ← ∅
3:     G′ ← copy of G
4:     while G′ contains at least one element which is not its own inverse do
5:         Add to S one such element and its inverse
6:         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 $G = \{a_1, \ldots, a_k, a_{k+1}, \ldots, a_n\}$. $G$ being abelian, we can rewrite $(a_1 \ldots a_n)^2$ as

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

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

5. $a_1 \ldots a_n = a_1 a_1^{-1} \ldots a_{\frac{n}{2}}\ a_{\frac{n}{2}}^{-1} = e$.

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

## 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**.

| | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

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 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.

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

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

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. $(g, h)(g, h) = (gg, hh) = (e_G, e_H) = e_{G \times H}$.

## 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. $G = \langle \mathbb{R}, \cdot \rangle$, $H = \{2^n 3^m : m, n \in \mathbb{Z}\}$. $H$ is a subgroup of $G$.
   (i) Suppose $2^n 3^m, 2^p 3^q \in H$; then $2^n 3^m 2^p 3^q = 2^{n+p} 3^{m+q}$. Since $n+p, m+q \in \mathbb{Z}$, $H$ is closed under multiplication.
   (ii) Suppose $2^n 3^m \in H$; then $(2^n 3^m)^{-1} = 2^{-n} 3^{-m}$. 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 $G$.
   (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 $a_i a_1, a_i a_2, \ldots, a_i a_n$ for some $a_i \in S$ and let us assume that $e \notin S$; then $a_i a_j \neq a_i$ for any $a_j \in S$. This observation, along with the fact that $G$ is a finite group, allows us to conclude that $a_i a_1 \neq a_i a_2 \neq \ldots \neq a_i a_n \neq a_i$. $S$ 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 $a_i a_j \neq e$ for any $a_j \in S$. Similar to the observation above, this would imply that $S$ has $n+1$ elements (all $a_i a_j$ 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 $xx^{-1}ax^{-1} \in H \Rightarrow a \in H$. 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 $(x_1, e)(x_2, e) = (x_1 x_2, e) \in G \times H$. 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 $(x_1, x_1)(x_2, x_2) = (x_1 x_1, x_2 x_2) \in G \times G$. 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.

| | $e$ | $a$ | $b$ | $b^2$ | $b^3$ | $ab$ | $ab^2$ | $ab^3$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $b^2$ | $b^3$ | $ab$ | $ab^2$ | $ab^3$ |
| $a$ | $a$ | $e$ | $ab$ | $ab^2$ | $ab^3$ | $b$ | $b^2$ | $b^3$ |
| $b$ | $b$ | $ab^3$ | $b^2$ | $b^3$ | $e$ | $a$ | $ab$ | $ab^2$ |
| $b^2$ | $b^2$ | $ab^2$ | $b^3$ | $e$ | $b$ | $ab^3$ | $a$ | $ab$ |
| $b^3$ | $b^3$ | $ab$ | $e$ | $b$ | $b^2$ | $ab^2$ | $ab^3$ | $a$ |
| $ab$ | $ab$ | $b^3$ | $ab^2$ | $ab^3$ | $a$ | $e$ | $b$ | $b^2$ |
| $ab^2$ | $ab^2$ | $b^2$ | $ab^3$ | $a$ | $ab$ | $b^3$ | $e$ | $b$ |
| $ab^3$ | $ab^3$ | $b$ | $a$ | $ab$ | $ab^2$ | $b^2$ | $b^3$ | $e$ |

Table 12: Operation table of the dihedral group $D_4$

3. See Table 13.
4. See Table 14.

## 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.

| | $e$ | $a$ | $b$ | $b^2$ | $b^3$ | $ab$ | $ab^2$ | $ab^3$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $b^2$ | $b^3$ | $ab$ | $ab^2$ | $ab^3$ |
| $a$ | $a$ | $b^2$ | $ab$ | $ab^2$ | $ab^3$ | $b^3$ | $e$ | $b$ |
| $b$ | $b$ | $ab^3$ | $b^2$ | $b^3$ | $e$ | $a$ | $ab$ | $ab^2$ |
| $b^2$ | $b^2$ | $ab^2$ | $b^3$ | $e$ | $b$ | $ab^3$ | $a$ | $ab$ |
| $b^3$ | $b^3$ | $ab$ | $e$ | $b$ | $b^2$ | $ab^2$ | $ab^3$ | $a$ |
| $ab$ | $ab$ | $b$ | $ab^2$ | $ab^3$ | $a$ | $b^2$ | $b^3$ | $e$ |
| $ab^2$ | $ab^2$ | $e$ | $ab^3$ | $a$ | $ab$ | $b$ | $b^2$ | $b^3$ |
| $ab^3$ | $ab^3$ | $b^3$ | $a$ | $ab$ | $ab^2$ | $e$ | $b$ | $b^2$ |

Table 13: Operation table for the quaternion group

| | $e$ | $a$ | $b$ | $c$ | $ab$ | $bc$ | $ac$ | $abc$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $ab$ | $bc$ | $ac$ | $abc$ |
| $a$ | $a$ | $e$ | $ab$ | $ac$ | $b$ | $abc$ | $c$ | $bc$ |
| $b$ | $b$ | $ab$ | $e$ | $bc$ | $a$ | $c$ | $abc$ | $ac$ |
| $c$ | $c$ | $ac$ | $bc$ | $e$ | $abc$ | $b$ | $a$ | $ab$ |
| $ab$ | $ab$ | $b$ | $a$ | $abc$ | $e$ | $ac$ | $bc$ | $c$ |
| $bc$ | $bc$ | $abc$ | $c$ | $b$ | $ac$ | $e$ | $ab$ | $a$ |
| $ac$ | $ac$ | $c$ | $abc$ | $a$ | $bc$ | $ab$ | $e$ | $b$ |
| $abc$ | $abc$ | $bc$ | $ac$ | $ab$ | $c$ | $a$ | $b$ | $e$ |

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

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

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

## Set F

1. The whole committee.
2. If $f$ is injective, then every element of $A$ must map to a different element of $A$. In other words, every element in $A$ is image of some other element in $A$. Therefore $f$ is surjective.
3. Let us assume that $f$ is not injective, which corresponds to saying that at least one element is the image of at least two different elements in the domain. In that case, the number of elements in the range would be smaller than the number of elements in $A$, contradicting the fact that $f$ is surjective. Therefore, $f$ is injective.
4. $f : \mathbb{Z} \to \mathbb{Z}$, defined by $f(x) = 2x$, is injective but not surjective.
   $f : \mathbb{R} \to \mathbb{Z}$, defined by $f(x) =$ the least integer greater than or equal to $x$, is surjective but not injective.
5. $n^n$ functions, out of which $n!$ functions are bijective.

## Set G

1. Let us assume that $f$ is not injective. That means that there are at least two distinct elements $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$. In that case, $g(f(x_1)) = g(f(x_2))$, contradicting the fact that $g \circ f$ is injective. Therefore, $f$ is injective.
2. Let us assume that $g$ is not surjective. That means that there is at least one element in $C$ that is not an image of any element in $B$ under $g$. Then that element cannot possibly be an image of any element in $A$ under $g \circ f$, contradicting the fact that $g \circ f$ is surjective. Therefore, $g$ is surjective.
3. Take $f, g : \mathbb{Z} \to \mathbb{Z}$, defined by $f(x) = 2x$ and $g(x) = -x$; then $(g \circ f)(x) = -2x$, which is not bijective, since odd numbers are not images under this function.
4. For every $x$, $f(x)$ is defined and so is $g(f(x)) = x$. Therefore $g = f^{-1}$ and $f$ is bijective.

## Set H

In the following items, $*$ means "any symbol", and $!x$ means "any symbol except $x$". $0$ is always the initial state and, in the diagrams, the green circle represents the acceptance state. All others are failure states.

1. $A = \{a, b, c, d\}$; $S = \{0, 1, 2, 3, 4\}$; machine table: see Table 20; diagram: see Figure 1.
2. $A = \{a, b, c, d\}$; $S = \{0, 1, 2, 3\}$; machine table: see Table 21; diagram: see Figure 2
3. $A = \{0, 1, 2, 3, 4\}$; $S = \{0, 1, 2, 3, 4\}$; machine table: see Table 22; diagram: see Figure 3

| Present state | a | !a |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 2 | 1 |
| 2 | 3 | 2 |
| 3 | 4 | 3 |
| 4 | 4 | 4 |

Table 20: State machine for input consisting of exactly 3 a's

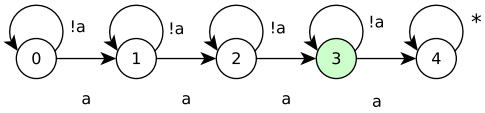



Figure 1: State machine for input consisting of exactly 3 a's

| Present state | a | !a |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 2 | 1 |
| 2 | 3 | 2 |
| 3 | 4 | 3 |
| 4 | 4 | 4 |

Table 21: State machine for input consisting of at least 3 a's

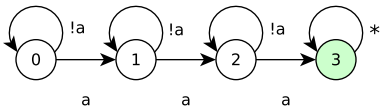



Figure 2: State machine for input consisting of at least 3 a's

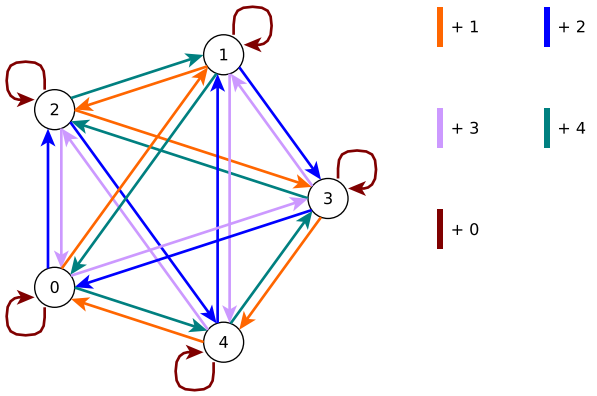



Figure 3: State machine for addition modulo 5

4. $A = \{0, 1\}$; $S = \{0, 1, 2, 3\}$; machine table: see Table 23; diagram: see Figure 4.

5. (a) $\bar{\alpha}(s_0, 000) = s_0 \quad \bar{\alpha}(s_0, 100) = s_1$
   $\bar{\alpha}(s_0, 001) = s_1 \quad \bar{\alpha}(s_0, 101) = s_0$
   $\bar{\alpha}(s_0, 010) = s_1 \quad \bar{\alpha}(s_0, 110) = s_0$
   $\bar{\alpha}(s_0, 011) = s_0 \quad \bar{\alpha}(s_0, 111) = s_1$

   (b) $\bar{\alpha}(s_0, 00) = s_0 \quad \bar{\alpha}(s_1, 00) = s_1$
   $\bar{\alpha}(s_0, 01) = s_1 \quad \bar{\alpha}(s_1, 01) = s_0$
   $\bar{\alpha}(s_0, 10) = s_1 \quad \bar{\alpha}(s_1, 10) = s_0$

| Present state | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

Table 22: State machine for addition modulo 5

| Present state | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 0 | 2 |
| 2 | 0 | 3 |
| 3 | 0 | 0 |

Table 23: State machine for binary string ending in 111

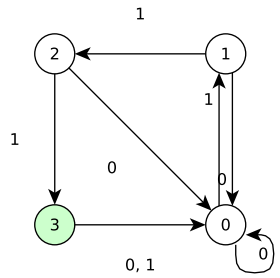



Figure 4: State machine for binary string ending in 111

$\bar{\alpha}(s_0, 11) = s_0 \quad \bar{\alpha}(s_1, 11) = s_1$

6. (a) $\mathbf{x} = 01001$: $T_{\mathbf{x}}(s_0) = s_0 \quad T_{\mathbf{x}}(s_1) = s_1$
   $\mathbf{x} = 10011$: $T_{\mathbf{x}}(s_0) = s_1 \quad T_{\mathbf{x}}(s_1) = s_0$
   $\mathbf{x} = 01010$: $T_{\mathbf{x}}(s_0) = s_0 \quad T_{\mathbf{x}}(s_1) = s_1$

   (b) In the case of $M_1$, $T_{\mathbf{x}}$ either maps the initial state to the same state if the weight of **x** is even and to the opposite state otherwise. So, there are only two functions.

   (c) In general, let $n$ be the number of $a$'s in a given **x**; then $T_{\mathbf{x}}(s_i) = s_j$, in which $j = \max(i + n, 4)$.

   (d) We can think of $T_{\mathbf{x}}(s_i)$ as a fuction $f(\mathbf{x}, i) = \sum_{b \in \mathbf{x}} (b \mod 4) + (i \mod 4)$. Since **x** determines the function and there are only 5 possible values for the term that includes it in $f$, there are therefore only 5 distinct transition functions in this case.

## Set I

1. see Table 24 and Figure 5.

| Present state | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Table 24: Automaton $M(\mathbb{Z}_4)$

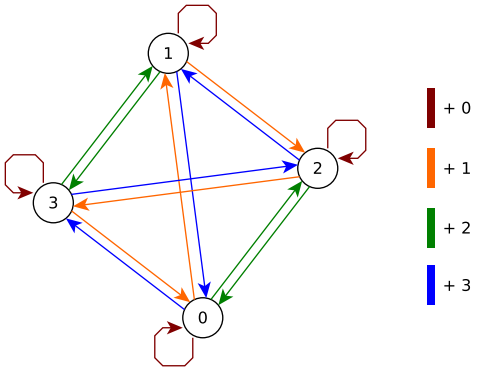
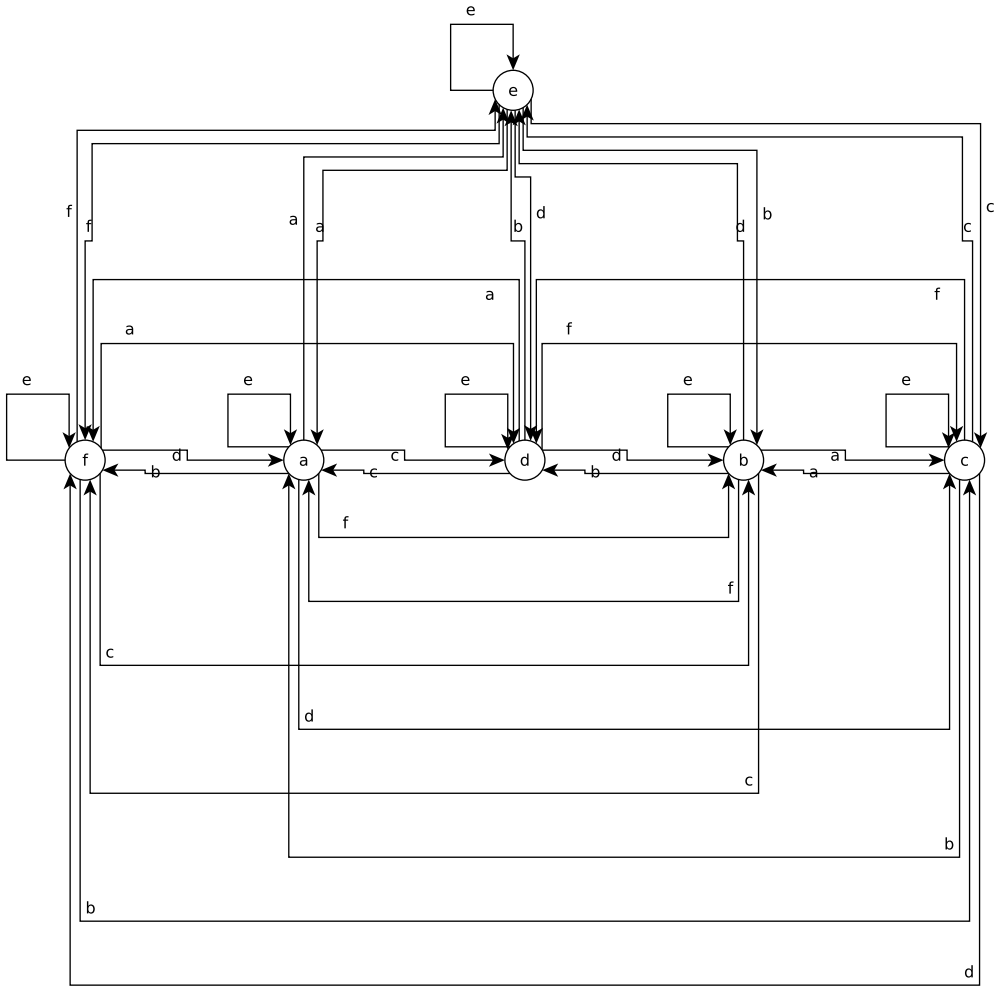



Figure 5: Automaton $M(\mathbb{Z}_4)$

2.

$$e = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$
$$a = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$
$$b = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$
$$c = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$
$$d = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$
$$f = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

| $\circ$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
| $a$ | $a$ | $e$ | $f$ | $d$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $d$ | $f$ | $e$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $e$ | $f$ | $d$ |
| $d$ | $d$ | $f$ | $e$ | $a$ | $b$ | $c$ |
| $f$ | $f$ | $d$ | $c$ | $b$ | $a$ | $e$ |




3. $(T_{\mathbf{y}} \circ T_{\mathbf{x}})(s_i) = \bar{\alpha}(\bar{\alpha}(s_i, \mathbf{x}), \mathbf{y})$. This corresponds to putting the automaton in the state $s_i$, then applying all the events in **x** and then applying all the events in **y**. Symbolically, $(T_{\mathbf{y}} \circ T_{\mathbf{x}})(s_i) = \bar{\alpha}(s_i, \mathbf{xy}) = T_{\mathbf{xy}}$.

4. As we've seen in exercise H5b of this chapter, there are only two transition functions for $M_1$. Let us call them $E(s_i) = s_i$ and $I(s_i) = s_{\text{inverse of } i}$. See Table 25 for the group operation of $\mathscr{S}(M_1)$. $E$ is the identity element and each element is the inverse of itself. So $\mathscr{S}(M_1)$ is also a group.

| $\circ$ | $E$ | $I$ |
|---|---|---|
| $E$ | $E$ | $I$ |
| $I$ | $I$ | $E$ |

Table 25: Operation table of $\mathscr{S}(M_1)$

5. As we've seen, there are only 5 transition functions in $M_2$. Let's call them $P_i$, for $0 \leqslant i \leqslant 4$, so that $P_i(s_j) = (i + j)$

mod 4. The operation table is essentially the same as Table 22. And it is also a group.

6. *The diagram shows multiple arrows for the same event leaving the same state. This is not a state machine.*

# Chapter 7

## Set A

1. $f^{-1} = \begin{bmatrix}1&2&3&4&5&6\\2&6&3&5&4&1\end{bmatrix}$ $g^{-1} = \begin{bmatrix}1&2&3&4&5&6\\3&1&2&6&5&4\end{bmatrix}$ $h^{-1} = \begin{bmatrix}1&2&3&4&5&6\\2&6&1&4&5&3\end{bmatrix}$
   $g \circ f = \begin{bmatrix}1&2&3&4&5&6\\4&2&1&5&6&3\end{bmatrix}$ $f \circ g = \begin{bmatrix}1&2&3&4&5&6\\1&3&6&2&4&5\end{bmatrix}$
2. $f \circ (g \circ h) = \begin{bmatrix}1&2&3&4&5&6\\6&1&5&2&4&3\end{bmatrix}$
3. $g \circ h^{-1} = \begin{bmatrix}1&2&3&4&5&6\\3&4&2&6&5&1\end{bmatrix}$
4. $h \circ g^{-1} \circ f^{-1} = \begin{bmatrix}1&2&3&4&5&6\\3&4&1&5&2&6\end{bmatrix}$
5. $g \circ g \circ g = \begin{bmatrix}1&2&3&4&5&6\\1&2&3&6&5&4\end{bmatrix}$

## Set B

1. $G$ is a group since the composition of functions is associative, there is an identity element, $\epsilon$, and each element is its own inverse. Operation table:

| $\circ$ | $\epsilon$ | $f$ | $g$ | $h$ |
|---|---|---|---|---|
| $\epsilon$ | $\epsilon$ | $f$ | $g$ | $h$ |
| $f$ | $f$ | $\epsilon$ | $h$ | $g$ |
| $g$ | $g$ | $h$ | $\epsilon$ | $f$ |
| $h$ | $h$ | $g$ | $f$ | $\epsilon$ |

2. $f = \begin{bmatrix}1&2&3&4&5&6\\2&3&4&1&6&5\end{bmatrix}$ $f^2 = \begin{bmatrix}1&2&3&4&5&6\\3&4&1&2&5&6\end{bmatrix}$ $f^3 = \begin{bmatrix}1&2&3&4&5&6\\4&1&2&3&6&5\end{bmatrix}$ $f^4 = \epsilon = \begin{bmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{bmatrix}$
3. $e = \begin{bmatrix}1&2&3&4&5\\1&2&3&4&5\end{bmatrix}$
   $f = \begin{bmatrix}1&2&3&4&5\\4&3&2&1&5\end{bmatrix}$
   $g = \begin{bmatrix}1&2&3&4&5\\2&1&4&3&5\end{bmatrix}$
   $h = \begin{bmatrix}1&2&3&4&5\\3&4&1&2&5\end{bmatrix}$

| $\circ$ | $e$ | $f$ | $g$ | $h$ |
|---|---|---|---|---|
| $e$ | $e$ | $f$ | $g$ | $h$ |
| $f$ | $f$ | $e$ | $h$ | $g$ |
| $g$ | $g$ | $h$ | $e$ | $f$ |
| $h$ | $h$ | $g$ | $f$ | $e$ |

4. **TODO**

## Set C

1. $f(g(x)) = \frac{1}{(1-(x-1)/x)} = x$ and $g(f(x)) = \frac{x/(1-x)}{1/(1-x)} = x$. Therefore $A$ is closed under composition and inverses.
2. Every function is its own inverse and $gf = fg = h$, $fh = hf = g$ and $gh = hg = f$. Therefore $A$ is closed under composition and inverses.
3. **TODO**
4. **TODO**

## Set D

1. $f_n : \mathbb{R} \to \mathbb{R}$ is bijective and its inverse is defined as $f_n^{-1}(x) = x - n$.
2. $f_n(f_m(x)) = x + m + n = f_{n+m}(x)$. $f_{-n}(f_n(x)) = x + n - n = x$. Therefore $f_{-n} = f_n^{-1}$.
3. $G$ is closed under composition and inverses (see previous item).
4. $f_1$ is a generator of $G$.

## Set E

1. $f_{a,b} : \mathbb{R} \to \mathbb{R}$ is bijective and its inverse is defined as $f_{a,b}^{-1}(x) = (x - b)/a$.
2. $f_{a,b}(f_{c,d}(x)) = f_{a,b}(cx + d) = a(cx + d) + b = acx + ad + b = f_{ac,ad+b}(x)$.
3. $f_{a,b}^{-1}(x) = (x - b)/a = (1/a)x - b/a = f_{1/a,-b/a}(x)$.
4. From the previous item we know that $G$ is closed under composition and inverses.

## Set F

1. $R_0 = \begin{bmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{bmatrix}$ $R_1 = \begin{bmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{bmatrix}$ $R_2 = \begin{bmatrix}1&2&3&4&5&6\\3&4&5&6&1&2\end{bmatrix}$
   $R_3 = \begin{bmatrix}1&2&3&4&5&6\\4&5&6&1&2&3\end{bmatrix}$ $R_4 = \begin{bmatrix}1&2&3&4&5&6\\5&6&1&2&3&4\end{bmatrix}$ $R_5 = \begin{bmatrix}1&2&3&4&5&6\\6&1&2&3&4&5\end{bmatrix}$
   $R_6 = \begin{bmatrix}1&2&3&4&5&6\\5&4&3&2&1&6\end{bmatrix}$ $R_7 = \begin{bmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{bmatrix}$ $R_8 = \begin{bmatrix}1&2&3&4&5&6\\1&6&5&4&3&2\end{bmatrix}$
   $R_9 = \begin{bmatrix}1&2&3&4&5&6\\2&1&6&5&4&3\end{bmatrix}$ $R_{10} = \begin{bmatrix}1&2&3&4&5&6\\3&2&1&6&5&4\end{bmatrix}$ $R_{11} = \begin{bmatrix}1&2&3&4&5&6\\4&3&2&1&6&5\end{bmatrix}$
2. $\epsilon = \begin{bmatrix}1&2&3&4\\1&2&3&4\end{bmatrix}$
   $a = \begin{bmatrix}1&2&3&4\\4&3&2&1\end{bmatrix}$
   $b = \begin{bmatrix}1&2&3&4\\2&1&4&3\end{bmatrix}$
   $c = \begin{bmatrix}1&2&3&4\\3&4&1&2\end{bmatrix}$

   | $\circ$ | $\epsilon$ | $a$ | $b$ | $c$ |
   |---|---|---|---|---|
   | $\epsilon$ | $\epsilon$ | $a$ | $b$ | $c$ |
   | $a$ | $a$ | $\epsilon$ | $c$ | $b$ |
   | $b$ | $b$ | $c$ | $\epsilon$ | $a$ |
   | $c$ | $c$ | $b$ | $a$ | $\epsilon$ |
3. **TODO**
4. **TODO**

## Set G

1. **TODO**
2. **TODO**
3. **TODO**
4. **TODO**

## Set H

1. Let $f, g \in G$; then $f(g(a)) = a$, which means that $f \circ g \in G$. And $f(a) = a \Rightarrow f^{-1}(a) = a$, so $f^{-1} \in G$. Therefore $G$ is a subgroup of $S_A$.
2. Let $f, g \in G$ so that $f$ and $g$ move $n$ and $m$ elements, respectively; then $f \circ g$ can move, at most, a finite number of elements (namely, $n + m$). And $f^{-1}$ maps the same number of elements as $f$. So $G$ is closed under composition and inverses and therefore is a subgroup of $S_A$.

3. Let $f, g \in G$; then $f(g(x)) \in B$ for any $x \in B$, so $f \circ g \in G$. And let's say $B$ has $n$ elements; then $f$ will map those elements of $B$ to $n$ different elements of $B$ (because $f$ is bijective). $f$ "exhausts" all elements of $B$, in the sense that there can be no element in $B$ that is not an image of $B$ under $f$. More formally, for any $x \in A$, $f(x) \in B \Rightarrow x \in B$. So $f^{-1} \in G$. Therefore $G$ is a subgroup of $S_A$.

4. Let us define a function $f : \mathbb{N} \to \mathbb{N}$ such that $f(n) = 2n$ if $n$ is even; if $n$ is odd, we "cover the holes" left by the even integers. So, the function looks like:

$$f = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \dots \\ 0 & 1 & 4 & 2 & 8 & 3 & 12 & 5 & 16 & \dots \end{bmatrix}$$

   $A = \mathbb{N}$ and $B = \{x \in \mathbb{N} : x = 2k, k \in \mathbb{N}\}$. It is clear that $f$ maps every even number to another even number. Due to the way it is constructed, $n_1 \neq n_2 \Rightarrow f(n_1) \neq f(n_2)$ (injective). The function definition also guarantees that any integer $m$ is the image of some integer $n$; $\mathbb{N}$ is infinite, so if we keep incrementing $x$, eventually it will map to $m$ (surjective). So $f$ is a permutation. But note, for example, that $f^{-1}(2) = 3$. So $f^{-1} \notin G$ and, therefore, $G$ is not a subgroup of $S_A$.

### Set I

1. $\alpha(k_i) = k_i = \epsilon(k_i)$. From (viii) we can conclude that $\alpha = \epsilon$.

2. We can think of this group as a directed graph in which the edges are the clans and, for any pair $(k_i, k_j)$, there is a directed vertex $k_i \to k_j$ if, and only if, $\alpha(k_i) = k_j$. This graph must have a cycle since: 1) every edge has an outgoing vertex (it's always possible to apply $\alpha$ to any edge) and 2) the set of clans is finite, so any sufficiently long path will eventually revisit some edge. In fact, the length of any cycle is no greater than $n$ (otherwise, that path would have more than $n$ *different* edges, which is impossible).

   So, take any cycle and any clan $k$ in that cycle. Let $m \leqslant n$ be the length of this cycle. Algebraically, we have $\alpha^m(k) = k = \epsilon(k)$. By (viii), $\alpha^m = \epsilon$.

3. From (vii) we can conclude that the number of permutations cannot be less than $n$ (otherwise, for any given clan $k_i$ there would be another clan $k_j$ so that people in $k_i$ would not have any relation in $k_j$) and it cannot be greater than $n$ either (otherwise it would result in more than $n$ clans, which is impossible). So the number of permutations is exactly $n$.

4. Let's say people in clan $k_i$ have children in clan $k_j$, that is, $c(k_i) = k_j$. So $c^{-1}(c(k_i)) = k_i = c^{-1} = (k_j)$. In other words, people in $k_j$ have fathers in $c^{-1}(k_j)$. Similarly for $w$.

5. If $c(k_i) = k_i$ then $c = \epsilon$ by (viii). If a woman is in clan $k_i$, then her husband lives in clan $w^{-1}(k_i)$ and their son lives in clan $c(w^{-1}(k_i)) = k_i = \epsilon(k_i)$. So $c \circ w^{-1} = \epsilon \Rightarrow c = w$.

6. $c \circ w^{-1} \circ w \circ c^{-1} = \epsilon$, which means that any man and his matrilateral parallel cousins are in the same clan. By (vi), such kind of marriage is prohibited.

7. **TODO**.

8. If a woman is in clan $k_i$ then the son of her mother's brother is in clan $c \circ w \circ c^{-1}(k_i)$. Her husband comes from that clan, so $w^{-1}(k_i) = c \circ w \circ c^{-1}(k_i)$. So $c \circ w \circ c^{-1} = w^{-1}$ and, therefore, $c \circ w = w^{-1} \circ c$.

9. If a woman is in clan $k_i$ then the son of her father's sister is in clan $c \circ w^{-1} \circ c^{-1}$. Her husband comes from that clan, so $c \circ w^{-1} \circ c^{-1} = w^{-1}$. Therefore $c \circ w^{-1} = w^{-1} \circ c$ .

## Chapter 8

### Set A

1. (a) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 7 & 5 & 1 & 8 & 3 & 2 \end{bmatrix}$

   (b) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 5 & 9 & 4 & 2 & 1 & 6 & 3 \end{bmatrix}$

   (c) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 6 & 9 & 7 & 3 & 1 & 2 & 4 \end{bmatrix}$

(d) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 7 & 5 & 6 & 3 \end{bmatrix}$

(e) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 2 & 6 & 5 & 1 & 7 & 4 \end{bmatrix}$

(f) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 9 & 2 & 1 & 7 & 6 & 8 \end{bmatrix}$

2. (a) $(145)(293)(67)$
   (b) $(17)(24)(395)(68)$
   (c) $(17435)(296)$
   (d) $(1928)(375)$

3. (a) $(18)(12)(14)(17)(13)$
   (b) $(28)(25)(23)(14)(16)$
   (c) $(57)(13)(12)(14)(16)$
   (d) $\pi = (76)(58)(12)(14)(13)$

4. (a) $(1, 2, 4)(3, 7)$
   (b) $(1, 2, 5, 3, 7, 4)$
   (c) $(1, 2)(4, 7)$
   (d) $(1, 7, 3, 5)$
   (e) $(1, 4, 2, 5, 3)$
   (f) $(1, 7, 4, 2, 3, 5)$
   (g) $(1, 2, 4, 3, 5)$
   (h) $(1, 4, 2, 7, 5)$

5. As a cycle:
   $(1, 2, 3, 4, 5)$
   $(2, 3, 4, 5, 1)$
   $(3, 4, 5, 1, 2)$
   $(4, 5, 1, 2, 3)$
   $(5, 1, 2, 3, 4)$

   As a product of transpositions:
   $(1, 5)(1, 4)(1, 3)(1, 2)$
   $(1, 5)(1, 4)(1, 3)(1, 2)(3, 4)(4, 3)$
   $(1, 5)(1, 4)(1, 3)(1, 2)(3, 5)(5, 3)$
   $(1, 5)(1, 4)(1, 3)(1, 2)(3, 2)(2, 3)$
   $(1, 5)(1, 4)(1, 3)(1, 2)(3, 1)(1, 3)$

6. (a) $\alpha = (1, 2, 3)$
   (b) $\alpha = (1, 4, 2, 5, 3)$
   (c) $\alpha = (1, 2, 3, 4)$

## Set B

1. (a) $\alpha^{-1} = (1, 3, 2)$
   $\alpha^2 = (1, 3, 2)$
   $\alpha^3 = ()$
   $\alpha^4 = (1, 2, 3)$
   $\alpha^5 = (1, 3, 2)$
   (b) $\alpha^{-1} = (1, 4, 3, 2)$
   $\alpha^2 = (1, 3)(2, 4)$
   $\alpha^3 = (1, 4, 3, 2)$
   $\alpha^4 = ()$
   $\alpha^5 = (1, 2, 3, 4)$

(c) $\alpha^{-1} = (1, 6, 5, 4, 3, 2)$
$\alpha^2 = (1, 3, 5)(2, 4, 6)$
$\alpha^3 = (1, 4)(2, 5)(3, 6)$
$\alpha^4 = (1, 5, 3)(2, 6, 4)$
$\alpha^5 = (1, 6, 5, 4, 3, 2)$

2. Each $\alpha^n$ corresponds to a permutation in which each element maps to the one $n$ "hops" ahead in the cycle. More formally, $\alpha^n(a_i) = a_{(i+n) \mod s}$. As a result there are $s$ different powers of $\alpha$.

3. $\alpha^{-1} = (a_s a_{s-1} \cdots a_1)$. From the equation in the previous item, $\alpha^{s-1}(a_i) = a_{(i+s-1) \mod s}$. So $\alpha^{s-1}(a_1) = a_s$, $\alpha^{s-1}(a_2) = a_1$ and so on. So $\alpha^{s-1} = (a_s a_{s-1} \cdots a_1) = \alpha^{-1}$.

4. Let us suppose $s$ is odd. If we start with $a_1$ and keep applying $\alpha^2$ repeatedly, we get $a_3, a_5, \ldots, a_s$, that is, all the elements with odd index. From then on, if we continue applying $\alpha^2$, we get $a_2, a_4, \ldots, a_{s-1}$, that is, all the elements with even index. With this procedure, we cover all the elements without repeating, thus forming a cycle. Now, if $s$ is even and we apply the same procedure, we only get odd numbers until we eventually return to $a_1$, forming a cycle that does not contain the whole domain (all the evens were left out). So, if $\alpha$ is a cycle, then $s$ is odd.

5. First, from the equation in item 2, $\alpha^{s+1}(a_i) = a_{(i+s+1) \mod s} = a_{(i+1) \mod s} = \alpha(a_i)$ for any $a_i$ in the domain. So $\alpha = \alpha^{s+1}$. If $s$ is odd, then $(s + 1)$ is divisible by 2. So, $(\alpha^{(s+1)/2})^2 = \alpha^{s+1} = \alpha$.

6. The reasoning here is similar to that in item 4; if $s$ is even and we apply $\alpha^2$ repeatedly starting from $a_1$, we'll generate all elements with odd index and come back to $a_1$, thus forming the cycle $(a_1 a_3 \ldots a_{s-1})$. Then, if we do the same, but starting from $a_2$, we'll cover all the even indices, forming the cycle $(a_2 a_4 \ldots a_s)$. These two cycles of length $s/2$ are disjoint and cover the whole domain, so $\alpha^2 = (a_1 a_3 \ldots a_{s-1})(a_2 a_4 \ldots a_s)$.

7. This is a generalization of the previous item; if $s = kt$ and we apply $\alpha^k$ repeatedly starting from $a_1$, we'll generate a cycle $c_1$, composed of the sequence of elements $a_i$ with $i = kj + 1$, for $0 \leqslant j \leqslant t - 1$. Similarly, starting from $a_2$, we generate a cycle $c_2$, composed of the sequence of elements $a_i$ with $i = kj + 2$, for $0 \leqslant j \leqslant t - 1$ and so on until $a_k$. All these cycles of length $s/k$ are disjoint and cover the whole domain, so $a^k = c_1 c_2 \ldots c_{s/k}$.

8. Let's start with element $a_i$ and apply $\alpha^n$ repeatedly, generating the sequence $a_i, a_{(i+n) \mod s}, a_{(i+2n) \mod s}$ and so on. In order for this sequence to form a cycle, for all $0 < j < s$, $jn \mod s$ must be non-zero. Since $\alpha^n = \alpha$, we know that $0 < n < s$. Now, let's assume that there are $j, n$ such that $jn \mod s = 0$, which means that $jn = sk$, for some integer $k$. $s$ cannot be one of the factors of $jn$ ($s$ is greater than both $j$ and $n$). So, if $jn$ can be factored at all, $jn = sk = f_1, f_2, \ldots, k, \ldots, f_m$. Dividing both sides by $k$, we can express $s$ as a product of intergers different from 1 and itself. In other words, $s$ is not prime. Therefore, if $s$ is prime, $\alpha^n$ is a cycle for any integer $n$.

## Set C

1. Even: (a) and (d) only.

2. For all subitems, we can start from the same observation: the product of two permutations (each one itself written a product of transpositions) can be represented by the simple concatenation of the two. So the number of transpositions that make up the product is the sum of the number of transpositions in each of the original permutations. Then:

   (a) Even plus even is even.

   (b) Odd plus odd is even.

   (c) Even plus odd is odd.

3. Any cycle $(a_1, a_2, \ldots, a_l)$ can be represented as the composition of transpositions $(a_1, a_{l-1})(a_1, a_{l-2}) \cdots (a_1, a_2)$. So, for a cycle of length $l$, the number of transpositions is $l - 1$. Therefore if $l$ is even, the composition is odd and vice-versa.

4. (a) From the previous item, we know that the $\alpha$ can be represented as a product of transpositions with size $l - 1$ and $\beta$ as a product of transpositions with size $m - 1$. And $\alpha\beta$ can be represented as a concatenation of the the these two. Therefore the size of this product is $l + m - 2$.

   (b) This is a generalization of item (a).

## Set D

1. This is a direct consequence of the fact that disjoint cycles commute.
2. Let's assume that at least one of $\alpha$ and $\beta$ is not the identity. In this case, $\alpha\beta(x) \neq x$ for all $x \in \{a_1, \ldots, a_s, b_1, \ldots, b_r\}$.
3. From item 1, $(\alpha\beta)^t = \alpha^t\beta^t$. Since $\alpha$ and $\beta$ are disjoint, so too are $\alpha^t$ and $\beta^t$. From item 2, $\alpha^t = \epsilon$ and $\beta^t = \epsilon$.
4. $\gamma = (a_s b_1)$, so that $\alpha\beta\gamma = (a_1, \ldots, a_s, b_2, \ldots, b_r, b_1)$.
5. $\gamma\alpha\beta = (b_2, \ldots, b_r, a_s, a_1, \ldots, a_{s-1}, b_1)$
   $\alpha\gamma\beta = (a_1, \ldots, a_s, b_1, \ldots, b_r)$.
6. **TODO**

## Set E

1. $\pi\alpha\pi^{-1}(\pi(a_1)) = \pi\alpha(a_1) = \pi(a_2)$. Analogously for $a_2, \ldots, a_s$.
2. Let $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$. Now let's choose any permutation $\pi$ such that $\pi(a_i) = b_i$ for any element in the cycle $\alpha$. Then, we can rewrite $\beta = (\pi(a_1), \ldots, \pi(a_n))$. From the previous item, we know, then, that $\beta = \pi\alpha\pi^{-1}$ and is, therefore, a conjugate of $\alpha$. The same reasoning applies in the other direction.
3. Let $\alpha = (a_1, \ldots, a_s)$ and $\beta = (b_1, \ldots, b_r)$. Taking any $\pi \in S_n$, $\pi\alpha\pi^{-1} = (\pi(a_1), \ldots, \pi(a_s))$ and $\pi\beta\pi^{-1} = (\pi(b_1), \ldots, \pi(b_r))$. Now suppose $\pi(a_i) = \pi(b_j)$ for some $i, j$. Since $\pi$ is a permutation, $a_i = b_j$, which is false, because $\alpha$ and $\beta$ are disjoint. Therefore $\pi\alpha\pi^{-1}$ and $\pi\beta\pi^{-1}$ are also disjoint.
4. $\pi\sigma\pi^{-1} = \pi\alpha_1\alpha_2\cdots\alpha_t\pi^{-1} = \pi\alpha_1\pi^{-1}\pi\alpha_2\pi^{-1}\cdots\pi\alpha_t\pi^{-1}$. Each $\pi\alpha_i\pi^{-1}$ is a cycle of the same length of $\alpha_i$ and they are all disjoint (see previous item).
5. Since $\alpha_1$ and $\alpha_2$ have the same length, it follows (from item 2) that they are conjugate, i.e., there is some permutation $\lambda$ such that $\alpha_1 = \lambda\alpha_2\lambda^{-1}$. Similarly, there is a permutation $\gamma$ such that $\beta_1 = \gamma\beta_2\gamma^{-1}$. Also from item 2, we know that we can construct $\lambda$ in such a way as to map elements in the cycle $\alpha_1$ to elements of $\alpha_2$ (elements from $\beta_1$ are mapped to themselves). Similarly, $\gamma$ maps from elements in $\beta_1$ to elements in $\beta_2$. Since $\alpha_1$ and $\beta_1$ are disjoint, we know (from item 3) that $\alpha_1\beta_1 = \lambda\alpha_2\lambda^{-1}\gamma\beta_2\gamma^{-1}$. But since $\gamma$ and $\lambda$ don't "modify" the same elements, we can rewrite the equation as $\alpha_1\beta_1 = \gamma\lambda\alpha_2(\gamma\lambda)^{-1}\gamma\lambda\beta_2(\gamma\lambda)^{-1}$. Making $\pi = \gamma\lambda$, we get $\alpha_1\beta_1 = \pi\alpha_2\beta_2\pi^{-1}$.

## Set F

1. From exercise 8.B.3, $\alpha^n(a_i) = a_{(i+n) \mod s}$ for any $a_i$ in the cycle. So $\alpha^s(a_i) = a_{(i+s) \mod s} = a_i$ and, therefore, $\alpha^s = \epsilon$. And $\alpha^{2s} = \alpha^s\alpha^s = \epsilon\epsilon = \epsilon$ and $\alpha^{3s} = \alpha^{2s}\alpha^s = \epsilon\epsilon = \epsilon$. $\alpha^k \neq \epsilon$ for all $k < s$, since it will always map an element in the cycle to a different element in the cycle.
2. This follows straighforwardly from item 1.
3. (a) 6
   (b) 4
   (c) 20
4. We need to find the smallest integer $n$ such that $(\alpha\beta)^n = \epsilon$. Since $\alpha$ and $\beta$ commute, $\alpha^n\beta^n = \epsilon$. And since they are disjoint, $\alpha^n = \epsilon$ and $\beta^n = \epsilon$. The order of $\alpha$ is 4, which means that $\alpha^{4p} = \epsilon$ for every integer $p \geqslant 1$. Similarly, the order of $\beta$ is 6, so $\beta^{6q} = \epsilon$ for every integer $q \geqslant 1$. So $n = 4p = 6q$. So the problem now has been reduced to find the least common multiple of 4 and 6, which is 12.
5. The least common multiple of $r$ and $s$ for the same reasons explained in the previous item.

### Set G

1. By definition, given any two different permutations $\alpha_i$ and $\alpha_j$, there is some $x$ such that $\alpha_i(x) \neq \alpha_j(x)$. Since $\beta$ is a permutation, there is some $y$ such that $\beta(y) = x$. So $\alpha_i\beta(y) \neq \alpha_j\beta(y)$ and, therefore, $\alpha_1\beta, \ldots, \alpha_r\beta$ are $r$ distinct permutations. That they are odd was already proved in exercise C2.

2. The proof that they are distinct is the same as in the previous item. That they are even was already proved in exercise C2.

3. Let's say the number of even permutations in $S_n$ is $r$ and the number of odd permutations is $s$. If we pick any odd permutation and mulitiply by each of the even permutations, we will get $r$ different odd permutations. So $s \geqslant r$. Similarly, if we get any odd permutation and multiply by each of the odd ones (including itself), we get $s$ different even permutations. So $r \geqslant s$. From these two inequalities, we can conclude that $r = s$, that is, the number of odd permutations is equal to the number of even permutations.

4. From C2, we know that the composition of two even permutations is even; so $A_n$ is closed under composition. And if we reverse the order of the cycles that compose to form a permutation, we get its inverse (that is, $\alpha_1\alpha_2 \ldots \alpha_n = (\alpha_n\alpha_{n-1} \ldots \alpha_1)^{-1}$, where $\alpha_i$ are cycles). So, clearly, the inverse of an even permutation is also even, that is $A_n$ is closed under inverses. Therefore $A_n$ is a subgroup of $S_n$.

5. There are only two possiblities: either $H$ contains only even permutations (of which $A_n$ is an example) or it contains at least one odd permutation. If the former is the case, there is nothing else to prove; if the latter is the case, then we can apply the same reasoning we did in exercise G3, just replacing $S_n$ with $H$.

### Set H

1. Every permutation can be written as a product of disjoint cycles and every cycle can be written as a product of transpositions. So every permutation can be written as a product of transpositions. In other words, the set of all transpositions in $S_n$ generates $S_n$.

2. Any cycle $(a_1, a_2, \ldots a_n)$ can be written as the product $(1, a_1)(1, a_n)(1, a_{n-1}) \ldots (1, a_1)$. Since any permutation can be written as a product of disjoint cycles, the set $\{(1, a_1), (1, a_2), \ldots (1, a_n)\}$ generates $S_n$.

3. Every permutation can be written as a product of transpositions of the form $(1, a_i)$ (see exercise H2). Given two elements $x, y$, $(1, x)(1, y) = (1, y, x)$. So we can get any even permutation, and apply this transformation to all consecutive transpositions in the product and the result will be a product of cycles of length 3. Therefore, the set of cycles of length 3 generates $A_n$.

4. *The hint says it all* B-)

5. *The hint says it all* B-)

## Chapter 9

### Set A

1. (a) injective: $f(a) = f(b) \Rightarrow \epsilon(a) = \epsilon(b)$.
   (b) surjective: $f(a) = a$, for every $a \in G$.
   (c) $f(ab) = \epsilon(ab) = \epsilon(a)\epsilon(b) = f(a)f(b)$.

2. (a) injective: $f^{-1}(a) = f^{-1}(b) \Rightarrow f(f^{-1}(a)) = f(f^{-1}(b)) \Rightarrow a = b$.
   (b) surjective: $f^{-1}(f(a)) = a$, for any $a \in G_1$.
   (c) $f^{-1}(f(a))f^{-1}(f(b)) = ab = f^{-1}(f(ab)) = f^{-1}(f(a)f(b))$, for any $a, b \in G_1$.

   item
   (a) injective: $g(f(a)) = g(f(b)) \Rightarrow f(a) = f(b) \Rightarrow a = b$.
   (b) surjective: $g$ is surjective, so for any $c \in G_3$ there exists some $b \in G_2$ such that $g(b) = c$. $f$ is surjective, so for any $b \in G_2$ there exists some $a \in G_1$ such that $f(a) = b$. Therefore, for any $c \in G_3$ there is some $a \in G_1$ such that $g(f(a)) = c$.
   (c) $g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b))$.

## Set B

1. For any $a \in G_1$, $f(e_1)f(a) = f(e_1 a) = f(a)$, Therefore, $f(e_1)$ is the neutral element $e_2 \in G_2$.
2. $e_2 = f(e_1) = f(aa^{-1}) = f(a)f(a^{-1}) \Rightarrow f^{-1}(a) = f(a^{-1})$.
3. Any $b \in G_1$ can be written as $b = a^n$, for some integer $n$. So every element of $G_2$ can be written as $f(a^n) = f^n(a)$.

## Set C

1. $G \ncong H$. In $G$, every element is its own inverse. In $H$, $i.i \neq 1$.
2. $G \ncong H$. In $\mathbb{Z}_4$, $1 + 1 = 2 \neq 0$.
3. $G \ncong H$. In $G$, every element is its own inverse. In $H$, $i.i \neq 1$.
4. $G \cong H$. $A = (23)$, $B = (123)$, $C = (13)$, $D = (132)$, $K = (12)$, $I = ()$.
5. **TODO**.
6. $G \ncong H$. In $G$, every element is its own inverse. In $H$, $i.i \neq 1$.

## Set D

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong P_2$. $f : P_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2, f = \begin{pmatrix} \varnothing & a & b & a,b \\ (0,0) & (0,1) & (1,0) & (1,1) \end{pmatrix}$.
   $\mathbb{Z}_4 \cong V$. $f : \mathbb{Z}_4 \to V, f = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & i & -1 & -i \end{pmatrix}$.
2. $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \cong \mathbb{Z}_7^*$. Each of these three groups is generated by a single element: $(1,1)$, $1$ and $3$, respectively. $S_3$ does not have this property, so it is not isomorphic to the other three groups.
3. $P_3$.
4. For this exercise, let's call the groups $A$, $B$, $C$ and $D$, respectively according to the order in which they appear in the book.

   $A$ and $B$ are generated by two elements each. In $A$, let's call them $a$ and $b$. From the diagrams we can deduce that $a^2 = b^3 = e$. In $B$, let's call them $c$ and $d$. Similarly, $c^2 = d^3 = e$. If they are to be isomorphic, a necessary condition is: any isomorphism between them maps $a \to c$ and $b \to d$. However, $ba = ab^2$ and $dc = cd$. If they were isomorphic, $dc$ would equal $cd^2$.

   $C$ also has two generators, $f$ and $g$. But $f^2 = g^2 = e$, which is different from $A$ and $B$. So $C$ is not isomorphic to any of them.

   $D$ has only one generator, so it's not isomorphic to any of the other groups.

## Set E

1. $f : \mathbb{Z} \to E, f(n) = 2n$.
   (a) injective: $f(a) = f(b) \Rightarrow 2a = 2b \Rightarrow a = b$.
   (b) surjective: by definition, for any $m \in E$, $m = 2k$, for some $k \in \mathbb{Z}$. So $f(k) = m$.
   (c) $f(a) + f(b) = 2a + 2b = 2(a + b) = f(a + b)$.
2. $f : \mathbb{Z} \to G, f(n) = 10^n$.
   (a) injective: $f(a) = f(b) \Rightarrow 10^a = 10^b \Rightarrow a = b$.
   (b) surjective: For any $m \in G$, $f(\log_{10} y) = y$.
   (c) $f(a)f(b) = 10^a.10^b = 10^{a+b} = f(a + b)$.
3. $f : \mathbb{R} \times \mathbb{R} \to \mathbb{C}, f(a, b) = a + bi$.
   (a) injective: $f(a, b) = f(c, d) \Rightarrow a + bi = c + di \Rightarrow a = c, b = d \Rightarrow (a, b) = (c, d)$.
   (b) surjective: by definition, for any $x = a + bi \in \mathbb{C}$, $f(a, b) = x$, for some pair $(a, b) \in \mathbb{R} \times \mathbb{R}$.

(c) $f(a,b) + f(c,d) = (a+bi) + (c+di) = (a+c) + (b+d)i = f(a+c, b+d)$.

4. In $\mathbb{R}^*$, $-1.(-1) = 1$, which is the identity element. In other words, $-1$ is a non-identity element that is its own inverse. In $\mathbb{R}$, there is no such element, because $x + x = 2x$. The only element that satisfies the equation $2x = 0$ is $x = 0$. Therefore, $\mathbb{R}^* \ncong \mathbb{R}$.

5. $\mathbb{Z}$ is generated by a single element, 1. There can be no single element that generates $\mathbb{Q}$. Let's prove this by contradiction, by assuming there is such a generator $\frac{a}{b}$. Then, for any other rational number, $\frac{c}{d}$, there is an integer $n$ such that $\frac{a}{b}.n = \frac{c}{d}$. For two rationals to be considered equal, $and = bc$. Since $b \neq 0$, we can rewrite this equation as $c = \frac{d}{b}an$. That means that all rational numbers whose denominators are not multiples of $b$ cannot be generated by $\frac{a}{b}$. Therefore, there is no single generator for $\mathbb{Q}$ and $\mathbb{Z} \ncong \mathbb{Q}$.

6. Let's assume that there is an isomorphism, $f : \mathbb{Q} \to \mathbb{Q}^{\mathbf{POS}}$. Being an isomorphism, there must exist some $a \in \mathbb{Q}$ such that $f(a) = 2$. Also,

$$f\left(\frac{a}{2} + \frac{a}{2}\right) = f\left(\frac{a}{2}\right) f\left(\frac{a}{2}\right) = \left[f\left(\frac{a}{2}\right)\right]^2 = 2$$

But there is no element in $\mathbb{Q}^{\mathbf{POS}}$ whose square is 2. Therefore, there is no isomorphism between $\mathbb{Q}$ and $\mathbb{Q}^{\mathbf{POS}}$.

## Set F

1. $f : G_1 \to G_2$ is an isomorphism in which $f((24)) = a$, $f((1234)) = b$:
$(24)^2 = (24)(24) = e$
$(1234)^4 = (1234)(1234)(1234)(1234) = e$
$(1234)(24) = (24)(1234)(1234)(1234) = (12)(34)$

2. $f : G \to G'$ is an isomorphism in which $f((23)) = a$ and $f((13)) = b$.

3. **TODO**

4. **TODO**

## Set G

1. (a) injective: $f(a) = f(b) \Rightarrow a - 1 = b - 1 \Rightarrow a = b$.
   (b) surjective: For any $y \in G$, $f(y + 1) = y$.
   (c) $f(a) * f(b) = a - 1 + b - 1 + ab - a - b + 1 = ab - 1 = f(ab)$.

2. $f : \mathbb{R} \to G, f(x) = x - 1$. This function is bijective for the same reasons shown in the previous exercise. In addition, $f(a) * f(b) = a - 1 + b - 1 + 1 = a + b - 1 = f(a + b)$.

3. $f(x) = 2x$.
   (a) injective: $f(a) = f(b) \Rightarrow 2a = 2b \Rightarrow a = b$.
   (b) surjective: $f(y/2) = y$ for any $y \in G$.
   (c) $f(a) * f(b) = \frac{2a2b}{2} = 2ab = f(ab)$.

4. (a) injective: $f(a,b) = f(c,d) \Rightarrow (-1)^b a = (-1)^d c$. Since $b$ and $c$ can only assume the values 0 and 1 and $a$and $c$ are both positive, we can conclude that $(a,b) = (c,d)$.
   (b) $f\left(|y|, \frac{-y+|y|}{2|y|}\right) = y$ for any $y \in G$.
   (c) $f(a,b).f(c,d) = (-1)^a b.(-1)^c d = (-1)^{a+c} bd = f(bd, a+c)$. Obs.: in the case $a = c = 1$, in $\mathbb{R}^*$, $a + c = 2$ and in $\mathbb{Z}_2$, $a + c = 0$. But in both cases, $(-1)^{a+c} = 1$, so the equality holds.

### Set H

1. $f : G \times H \to H \times G, f(a, b) = (b, a)$ is an isomorphism.
   (a) $f(a, b) = f(c, d) \Rightarrow (b, a) = (d, c) \Rightarrow (a, b) = (c, d)$.
   (b) surjective: $f(b, a) = (a, b)$ for any $(a, b) \in H \times G$.
   (c) $f(a, b)f(c, d) = (b, a)(d, c) = (bd, ac) = f(ac, bd)$.
2. Let $g : G_1 \to G_2$ and $h : H_1 \to H_2$ be isomophisms. Then $f(a, b) = (g(a), h(b))$.
   (a) injective: $f(a, b) = f(c, d) \Rightarrow (g(a), h(b)) = (g(c), h(d)) \Rightarrow g(a) = g(c)$ and $h(b) = h(d)$. Since $g$ and $h$ are isomophisms, $a = c$ and $b = d$. So $(a, b) = (c, d)$.
   (b) surjective: $f(g^{-1}(a), h^{-1}(b)) = (a, b)$ for any $(a, b) \in G_2 \times H_2$.
   (c) $f(a, b)f(c, d) = (g(a), h(b))(g(c), h(d)) = (g(a)g(c), h(b)h(d))$. Since $g$ and $h$ are isomophisms, $g(a)g(c) = g(ac)$ and $h(b)h(d) = h(bd)$. So, $f(a, b)f(c, d) = (g(ac), h(bd)) = f(ac, bd)$.
3. First, let's assume that $f(x) = x^{-1}$ is an isomorphism from $G$ to $G$. Then, for any $a, b \in G$:
$$f(a)f(b) = f(ab) \Rightarrow a^{-1}b^{-1} = (ab)^{-1} \Rightarrow (ba)^{-1} = (ab)^{-1} \Rightarrow ba = ab$$
   Therefore, $G$ is abelian. To prove the opposite direction, we can simply make the inferences above in the reversse order.
4. $f : G \to H, f(x) = x^{-1}$.
   (a) injective: $f(a) = f(b) \Rightarrow a^{-1} = b^{-1} \Rightarrow a = b$.
   (b) surjective: $f(y^{-1}) = y$ for any $y \in H$.
   (c) $f(a) * f(b) = a^{-1} * b^{-1} = b^{-1}a^{-1} = (ab)^{-1}$.

### Set I

1. Since all elements of $\mathbb{Z}_6$ appear in the second row without repetition, $f$ is bijective. $f$ can be written as $f(x) - x$. So,
$$f(a) + f(b) = -a + (-b) = -(a + b) = f(a + b)$$
2. $f_3(x) = -x$. This is an automorphism for the same reason as the previous item.
   $f_1(x) = 2x$. $f_1(a) + f_1(b) = 2a + 2b = 2(a + b) = f(a + b)$.
   $f_2(x) = 3x$. $f_1(a) + f_1(b) = 3a + 3b = 3(a + b) = f(a + b)$.
3. (a) injective: $f(x) = f(y) \Rightarrow axa^{-1} = aya^{-1} \Rightarrow x = y$.
   (b) $f(a^{-1}ya) = y$ for any $y \in G$.
   (c) $f(x)f(y) = axa^{-1}aya^{-1} = axya^{-1} = f(xy)$.
4. For any $z \in G$ there is a $y \in G$ such that $g(y) = z$ because $g$ is an automorphism.
   For any $y \in G$ there is a $x \in G$ such that $f(x) = y$ because $f$ is an automorphism.
   Therefore, for any $z \in G$ there is a $x$ such that $f(g(x)) = z$.
   So, Aut$(G)$ is closed under composition. From exercise 9.A.2 we know that if $f$ is an isomophism, then $f^{-1}$ is also an isomophism. So Aut$(G)$ is also closed under inverses. Therefore, Aut$(G)$ is a subgroup of $S_G$.

## Chapter 10

### Set A

1. (a) $a^m a^n = a^0 a^n = ea^n = a^n = a^{0+n} = a^{m+n}$.
   (b) $m = -p$ for some $p > 0$. So,
   $a^m = a^{-p} = (a^{-1})^p$
   $a^n = (a^{-1})^{-n}$
   Therefore, $a^m a^n = (a^{-1})^p (a^{-1})^{-n} = (a^{-1})^{p-n} = a^{-p+n} = a^{m+n}$.

(c) $m = -k$, $n = -l$, for some $k, l > 0$. So,
$a^m = a^{-k} = (a^{-1})^k$
$a^n = a^{-l} = (a^{-1})^l$
Therefore, $a^m a^n = (a^{-1})^k (a^{-1})^l = (a^{-1})^{k+l} = a^{-(k+l)} = a^{m+n}$.

2. (a) $(a^m)^n = (a^0)^n = e^n = e = e^{0n} = e^{mn}$.
   (b) $(a^m)^n = (a^m)^0 = e = e^{0n} = e^{mn}$.
   (c) $m = -p$ for some $p > 0$. So,
   $(a^m)^n = (a^{-p})^n = ((a^{-1})^p)^n = \underbrace{\underbrace{a^{-1} \dots a^{-1}}_{p \text{ times}} \dots \underbrace{a^{-1} \dots a^{-1}}_{p \text{ times}}}_{n \text{ times}} = (a^{-1})^{pn} = a^{-pn} = a^{mn}$.
   (d) $n = -q$, for some $q > 0$.
   $(a^m)^n = (a^m)^{-q} = ((a^m)^{-1})^q = ((a^{-1})^m)^q$. Doing the same transformations as above, we get that $(a^m)^n = a^{mn}$.
   (e) $m = -p$, $n = -q$ for some $p, q > 0$. So,
   $(a^m)^n = (a^{-p})^{-q} = ((a^{-p})^{-1})^q = (a^p)^q = a^{pq} = a^{mn}$.

3. (a) $(a^n)^{-1} = (a^0)^{-1} = e^{-1} = e = a^{0.-1} = a^{n.-1} = a^{-n}$.
   (b) $(a^n)^{-1} = (a^{-q})^{-1} = a^q = a^{-n}$.

## Set B

1. $\text{ord}(10) = 5$, because $10.1 = 10$, $10.2 = 20$, $10.3 = 5$, $10.4 = 15$ and $10.5 = 0$.
2. $\text{ord}(6) = 8$, becaue $6.1 = 6$, $6.2 = 12$, $6.3 = 2$, $6.4 = 8$, $6.5 = 14$, $6.6 = 4$, $6.7 = 10$ and $6.8 = 0$.
3. $\text{ord}(f) = 4$. Same process as above.
4. $\text{ord}(1) = 1$ in $\mathbb{R}^*$. $\text{ord}(1) = \infty$ in $\mathbb{R}$.
5. $$f^2(x) = \frac{\frac{x}{2-x}}{2 - \left(\frac{x}{2-x}\right)} = \frac{\frac{x}{2-x}}{\frac{2(2-x)-x}{2-x}} = \frac{x}{2(2-x)-x}$$

   In general, the numerator will stay the same and the denominator can be described by the following recursive function:

   $$d^n(x) = 2d^{n-1}(x) - x$$

   The non-recursive version of this function is:

   $$d^n(x) = 2^n(1-x) + x$$

   Let's prove this by induction. For the base case ($n = 1$), we have:

   $$d^1(x) = 2^1(1-x) + x = 2 - 2x + x = 2 - x$$

   For the induction step, assume that $d^n(x) = 2^n(1-x) + x$. Then:

   $$d^{n+1}(x) = 2(2^n(1-x) + x) - x = 2^{n+1} + 2x - x = 2^{n+1}(1-x) + x$$

   Thus,

   $$f^n(x) = \frac{x}{d^n(x)} = \frac{x}{2^n(1-x) + x}$$

   In order for $f^n(x) = x$ for any $x \in A$, $d^n(x) = 1$ for any $x \in A$. So,

   $$2^n(1-x) + x = 1 \Rightarrow 2^n(1-x) = 1 - x \Rightarrow 2^n = 1 \Rightarrow n = 0$$

   Since the only solution to the equation is $n = 0$, $\text{ord}(f) = \infty$.

6. Yes, in every group (finite or infinite), $\text{ord}(e) = 1$.

7. (a) 12
   (b) 8, 16
   (c) 6, 18
   (d) 4, 20

## Set C

1. $\text{ord}(a) = 1 \Rightarrow a^1 = e \Rightarrow a = e$. Conversely, $e^1 = e \Rightarrow \text{ord}(e) = 1$.

2. $a^{n-r} = a^n a^{-r} = ea^{-r} = a^{-r} = (a^r)^{-1}$.

3. Let's say $\text{ord}(a) = n$. Then, $nm = k$, for some integer $m$. Since $k$ is odd, it can be written as $k = 2p + 1$ for some integer $p$. Let's assume $n$ is even, which means it can be written as $n = 2q$ for some integer $q$. Replacing all the variables:

$$nm = k \Rightarrow 2qm = 2p + 1$$

   which is impossible. Therefore, $\text{ord}(a)$ is odd.

4. Let's say $\text{ord}(bab^{-1}) = n$. Then, $\underbrace{bab^{-1} \dots bab^{-1}}_{n \text{ times}} = ba^n b^{-1} = e$. Multiplying both sides on the left by $b^{-1}$ and on the right by $b$: $a^n = e$. Now let's assume there is another integer $m < n$ such that $a^m = e$. Then $ba^m b^{-1} = e$, contradicting our premise that $\text{ord}(bab^{-1}) = n$. So $n$ is the smallest exponent of $a$ to yield $e$ and, therefore, $\text{ord}(a) = n = \text{ord}(bab^{-1})$.

5. Let's say $\text{ord}(a) = n$. Then $a^n = e \Rightarrow a^n a^{-n} = a^{-n} \Rightarrow (a^{-1})^n = e$. Also, $n$ is the smallest positive power of $a$ that is equal to $e$ for an analogous reason given in the previous exercise.

6. This is a generalization of the previous two exercises. The proof follows the same pattern.

## Set D

1. Let $\text{ord}(a) = n$. Then $p = nk$ for some integer $k$ (by theorem 5 of the chapter). Since $a \neq e$, $n \neq 1$. Because $p$ is prime, $k = 1$ and, therefore $p = n$.

2. Let $\text{ord}(a) = n$. Then $(a^k)^n = (a^n)^k = e^k = e$. By theorem 5, we know that $n$ is a multiple of the order of $a^k$.

3. $km$ is the smallest positive exponent of $a$ that yields $e$. It may be possible to rewrite $km$ as a different product of two integers, but if we fix $k$, then the other number cannot be smaller than $m$. Therefore, $m$ is the smallest exponent of $a^k$ that yields $e$, that is, $\text{ord}(a^k) = m$.

4. Let's first consider the case in which $a \neq e$. By the definition of odd number, $n = 2k + 1$ for some integer $k$. So,

$$e = a^{2k+1} = a^{2k}a \Rightarrow (a^2)^k = a^{-1} \Rightarrow \text{ord}(a^2) \neq k$$

   By theorem 5, the next exponent that yields $e$ is $2n$. So, $(a^2)^n = e \Rightarrow \text{ord}(a^2) = n$.
   In the case in which $a = e$, $\text{ord}(a^2) = \text{ord}(a) = 1$.

5. $a^n = a^{r-s} = e$. By theorem 5, $n$ is a multiple of $r - s$.

6. Let's start by denying the conclusion and assuming that $a$ is not in the center of $G$, that is, there is some integer $x$ such that $ax \neq xa$. Thus, $a \neq xax^{-1}$. But we know that $\text{ord}(a) = \text{ord}(xax^{-1}) = k$, which means that $a$ is not the only element in $G$ that has order $k$ (i.e., there are at least two: $a$ and $xax^{-1}$).

7. Again, let's deny the conclusion by assuming that $\text{ord}(a^k) = mp$ for some integer $p$. By part 2, we also know that $\text{ord}(a^k)q = \text{ord}(a)$ for some integer $q$. So, $mpq = \text{ord}(a)$, contradicting the hypothesis.

8. $a^{mk} = e$ and $a^{rk} = e$. By theorem 5, $mkp = rk$ for some integer $p$. Dividing by $k$ on both sides: $mp = r$.

## Set E

1. By theorem 5, $a^{np} = b^{mq} = e$ for any positive integers $p, q$. As a consequence, $a^{np}b^{mq} = e$. If we choose $p$ and $q$ such that $np = mq = k$, then $(ab)^k = e$ (because $a$ and $b$ commute). By definition, the smallest value of $k$ is $\text{lcm}(m, n)$. Therefore, $\text{ord}(ab) = \text{lcm}(m, n)$.

2. Let's assume that there exist positive integers $k, l$ such that $a^k = b^l \neq e$. Then $\text{ord}(a^k) = \text{ord}(b^l) \neq 1$. By exercise D2, we know that there exist positive integers $p, q$ such that:

$$\text{ord}(a^k)p = m$$
$$\text{ord}(b^l)q = n$$

   So $m$ and $n$ have a common divisor, $\text{ord}(a^k) = \text{ord}(b^l)$, different from $\pm 1$. In other words, they are not relatively prime.

3. Let's assume there are $i, j, k, l$ such that $i \neq k$, $j \neq l$ and $a^i b^j = a^k b^l$. Then $a^{k-i} = b^{j-l}$. From the previous exercise we can conclude that $m$ and $n$ are not relatively prime.

4. For some positive integer $k$:

| | |
|---|---|
| $\text{ord}(ab)k = \text{lcm}(m, n)$ | by part 1 |
| $\text{ord}(ab)k = mn$ | because $m$ and $n$ are relatively prime |
| $(ab)^{mn} = e$ | by theorem 5 |

   Let's assume that there is a positive integer $p$ such that $p < m$ and $(ab)^p = e$. Then

$$e = (ab)^p = a^p b^p \qquad \text{because } a \text{ and } b \text{ commute}$$
$$a^p = b^{-p}$$

   which contradicts the conclusion of part 2. Therefore $mn$ is the order of $ab$.

5. $\text{ord}(a) = m = \text{gcd}(m, n)p$ for some integer $p$. So $\text{ord}(a^{\text{gcd}(m,n)}) = p$. Since $a^{\text{gcd}(m,n)}$ and $b$ commute and $p$ is relatively prime to $n$:

$$\text{ord}(a^{gcd(m,n)}b) = pn = \frac{m}{\text{gcd}(m, n)}n = \text{lcm}(m, n)$$

   Therefore, $c = a^{gcd(m,n)}b$.

6. Consider the group of matrices in page 29 of the book. $A$ and $B$ do not commute, $\text{ord}(A) = 2$, $\text{ord}(B) = 3$ and $\text{ord}(AB) = \text{ord}(C) = 2 \neq 6 = \text{lcm}(2, 3)$.

## Set F

1. By theorem 5, $a$ to the power of every multiple of $12$ is equal to $e$. So what we are looking for is the smallest multiple of $8$ that is equal to some multiple of $n$. In other words, we are looking for the positive integer $k$ such that $8k = \text{lcm}(8, 12) = 24$. Therefore $k = 3$.

2. $\text{ord}(a) = 12 = 4.3$. By exercise D3, $\text{ord}(a^4) = 3$. Since $3$ is odd, by exercise D4, $\text{ord}((a^4)^2) = \text{ord}(a^8) = 3$.

3. Let $\text{ord}(a) = n$. Generalizing exercise F1, to find the order of $a^k$ corresponds to finding the smallest $j$ such that $(a^k)^j = a^{kj} = e$. By theorem 5 we know that $a^{in} = e$ for every positive integer $i$. So we need to find $j$ such that $kj = \text{lcm}(k, n)$. Then:

$$\text{ord}(a^k) = j = \frac{\text{lcm}(k, n)}{k} = \frac{kn}{\text{gcd}(k, n)k} = \frac{n}{\text{gcd}(k, n)} = \frac{\text{ord}(a)}{\text{gcd}(k, \text{ord}(a))}$$

   Using this result, we can calculate $\text{ord}(a^9) = 4$, $\text{ord}(a^{10}) = 6$, $\text{ord}(a^5) = 12$.

4. $5$, $7$ and $11$.

5. Already proved in exercise F3.

6. For all values of $k$ that are relatively prime to $\text{ord}(a)$.

## Set G

1. By exercise F3:

$$\text{ord}(a^m) = \frac{n}{\gcd(m,n)} = \frac{n}{1} = n$$

2. $$n = \frac{n}{\gcd(m,n)} \Rightarrow \gcd(m,n) = 1$$

3. Because $k$ is the order of $a^m$.

4. By theorem 5, $t = \frac{n}{\gcd(m,n)}p$ for some positive integer $p$. Then:

$$mt = \frac{m}{\gcd(m,n)}np$$

   Since $\frac{m}{\gcd(m,n)}$ is an integer, $n$ is a factor of $mt$.

5. Already proved in exercise F3.

## Set H

1. $\text{ord}(b^3) = \frac{\text{ord}(b)}{\gcd(3,\text{ord}(b))} = 12 \Rightarrow \text{ord}(b) = 12.\gcd(3,\text{ord}(b))$. Because 3 is prime, $\gcd(3,\text{ord}(b))$ is either 1 or 3. Let's assume it's 1; then $\text{ord}(b) = 12$. But $\gcd(3,12) = 3$, contradicting this hypothesis. So, $\text{ord}(b) = 36$.

2. Following the same reasoning above, $\text{ord}(b) = 24$.

3. Following the same reasoning above, $\text{ord}(b) = 60$.

4. $\text{ord}(b^k) = \frac{\text{lcm}(k,\text{ord}(b))}{k} = n \Rightarrow \text{lcm}(k,\text{ord}(b)) = l\,\text{ord}(b) = nk$ for some positive integer $l$. Therefore the order of $b$ is a factor of $nk$.

5. $b^{n'k} = e$. For the same reason, $b^{nk} = e$. So $b^{n'k} = b^{nk} \Rightarrow n = n'$, which is a contradiction.

6. $\text{ord}(b) = \frac{nk}{l}$, in which $n$ and $l$ are relatively prime. If $l > 1$, it is not a factor of $n$ and therefore it's not a prime factor of $k$. In this case, $l$ does not divide either $k$ or $n$. But $\text{ord}(b)$ is an integer, so $l = 1$ and $\text{ord}(b) = nk$.

# Chapter 11

## Set A

1. $\langle 6\rangle = \{0, 6, 12, 2, 8, 14, 4, 10\}$

2. $\langle f\rangle = \{(), (1642), (14)(26), (1246)\}$

3. $\langle \frac{1}{2}\rangle = \{x \in \mathbb{R}^* : x = \frac{1}{2^i}, i \in \mathbb{Z}\}$; $\langle \frac{1}{2}\rangle = \{x \in \mathbb{R} : x = \frac{i}{2}, i \in \mathbb{Z}\}$

4. $\langle f\rangle = \{g \in S_{\mathbb{R}} : g(x) = x + i, i \in \mathbb{Z}\}$

5. $\langle f\rangle = \{g \in \mathscr{F}(\mathbb{R}) : g(x) = x + i, i \in \mathbb{Z}\}$

6. Every element $n \in \mathbb{Z}$ can be written as $n = 1.n = (-1)(-n)$. Let's say $a \neq \pm 1 \in \mathbb{Z}$ is a generator of $\mathbb{Z}$. Then, for any $n_1, n_2 \in \mathbb{Z}$, $n_1 = ap_1$ and $n_2 = ap_2$ for some integers $p_1, p_2$. In this case, any two different integers would have a common divisor different from $\pm 1$, which is clearly not the case. So $1$ and $-1$ are the only generators of $\mathbb{Z}$. Every infinite cyclic group is isomorphic to $\mathbb{Z}$. So, only $a$ and $a^{-1}$ are the generators of $\langle a\rangle$.

7. By Cantor's diagonal argument, there is no bijective function from $\mathbb{R}^*$ to $\mathbb{Z}$. Therefore $\mathbb{R}^*$ is not cyclic.

## Set B

1. $G$ has an element of order $n$. Then, by theorem 3 of chapter 10, $G$ has $n$ different elements.

   $G$ has order $n$ and is generated by $a$. Then there exist $n$ different powers of $a$ and, therefore, ord$(a) = n$.

2. Let $G$ be a cyclic group generated by $a$ and let $b, c \in G$. Then $b = a^i$ and $c = a^j$ for some positive integers $i, j$. So $bc = a^i a^j = a^j a^i = cb$.

3. $b = a^k$ for some positive integer $k$, which implies that ord$(b) =$ ord$(a^k)$. By exercise 10.D.2, the order of $a^k$ (and therefore the order of $b$) is a factor of the order of $a$.

4. If $k$ divides $n$ then there is some integer $p$ such that $n = pk$. Let $a$ be the generator of the group. So ord$(a) = ord(pk)$ and, therefore, ord$(a^p) = k$.

5. Let $a, b \in G$ such that ord$(a) = m$ and ord$(b) = n$. Then ord$(ab) = mn$, because $m$ and $n$ are relatively prime and $a$ and $b$ commute ($G$ is abelian). Since the order of $G$ is $mn$, $ab$ is its generator and, therefore, $G$ is cyclic.

6. Let $b, c \in \langle a \rangle$. Then $b = a^i$ and $c = a^j$ for some integers $i, j$. So $f(b) = f(c) \Rightarrow a^{im} = a^{jm} \Rightarrow i = j \Rightarrow b = c$. So $f$ is an injective function. Since domain and codomain are the same in this case, it's also surjective.

   In addition, $f(a)f(b) = a^m b^m = (ab)^m = f(ab)$. Therefore, $f$ is an automorphism.

## Set C

1. ($\Rightarrow$) $a^r$ is a generator of $\langle a \rangle$. Then ord $a^r = n$. Then $r$ and $n$ are relatively prime. (see 10.G.2).

   ($\Leftarrow$) $r$ and $n$ are relatively prime. Then ord$(a^r) = n$ (see 10.G.1). Then $a^r$ is a generator of $\langle a \rangle$

2. Every $a^i$, such that $i < n$ and $i$ is relatively prime to $n$, is a generator of $\langle a \rangle$ by 11.C.1. By definition, there are $\phi(n)$ such powers of $a$.

3. $a, b \in C_m \Rightarrow (ab)^m = a^m b^m = e$ (closed under multiplication). $x \in C_m \Rightarrow (x^{-1})^m = (x^m)^{-1} = e^{-1} = e$ (closed under inverses).

4. Since $m$ divides $n$, by 11.B.4, there is an element $b \in \langle a \rangle$ with order $m$. So $b^1, b^2, \ldots, b^m \in C_m$.

5. ($\Rightarrow$) ord$(x) = m \Rightarrow x^m = e \Rightarrow x \in C_m$. So, for every integer $i$, $x^{im} = e$, which means that $x^i \in C_m$. $|\langle x \rangle| = m$ and $C_m$ has $m$ elements. So $\langle x \rangle = C_m$.

   ($\Leftarrow$) $x$ is a generator of $C_m$, which has $m$ elements. So $x^1, x^2, \ldots, x^m$ are all different. The smallest positive $i$ such that $x^i = e$ is $i = m$. In other words, ord$(x) = m$.

6. Take a generator $x$ of $C_m$. Then ord$(x) = m$. By 11.C.2 there are $\phi(m)$ different generators of $C_m$. All of them have order $m$. Therefore there are $\phi(m)$ elements of order $m$ in $\langle a \rangle$.

7. ($\Rightarrow$) $m =$ ord$(a^r) = \frac{mk}{\gcd(r, mk)} \Rightarrow \gcd(r, mk) = k \Rightarrow r = kl$.

   ($\Leftarrow$) $a^r = a^{kl} \Rightarrow$ ord$(a^r) = \frac{n}{\gcd(r,n)} = \frac{mk}{\gcd(kl, mk)} = \frac{mk}{k} = m$.

8. This is essentially a restatement of 11.C.1.

## Set D

1. $\langle a \rangle$ contains all powers of $b$ including $b^k = a$. Since $\langle b \rangle$ is a subgroup if $G$, any power of $a$ is also in $\langle b \rangle$. So $\langle a \rangle \subseteq \langle b \rangle$.

2. ($\Rightarrow$) By 11.D.1, if $a$ is a power of $b$ then $\langle a \rangle \subseteq \langle b \rangle$. Likewise, if $\langle b \rangle$ is a power of $\langle a \rangle$, then $\langle b \rangle \subseteq \langle a \rangle$. Therefore $\langle a \rangle = \langle b \rangle$.

   ($\Leftarrow$) $\langle a \rangle = \langle b \rangle$, so they have the same elements. Thus, $a \in \langle b \rangle$ and, since $\langle b \rangle$ is cyclic, $a = b^k$. Likewise for $b$.

3. ($\Rightarrow$) $\langle a \rangle = \langle b \rangle$. Then $|\langle a \rangle| = |\langle b \rangle| \Rightarrow$ ord$(a) =$ ord$(b)$.

   ($\Leftarrow$) ord$(a) =$ ord$(b) \Rightarrow |\langle a \rangle| = |\langle b \rangle|$. Since all cyclic groups of the same order are isomorphic, $\langle a \rangle = \langle b \rangle$.

4. (a) ord$(b) =$ ord$(a^k) = \frac{n}{\gcd(n,k)} = n \Rightarrow \gcd(k, n) = 1$. Therefore $k$ and $n$ are relatively prime. Apply the deduction above in the reverse order as well.

5. Same reasoning as the previous exercise.

6. By 11.B.4, there is an element in the group, call it $a$, such that ord$(a) = n$. The cyclic group $\langle a \rangle$ is a subgroup of order $n$.

### Set E

1. If $(a, b)$ is a generator of $G \times H$, then every element of $G \times H$ can be written as $(a, b)^k = (a^k, b^k)$ for some integer $k$. Now suppose there is an element $c \in G$ such that $c = a^k$ for every integer $k$. Then there is an element $(c, x) \in G$ that is not of the form $(a^k, b^k)$, which is a contradiction. Likewise for $b$.

2. Same reasoning as above. If $G \times H = \langle (a, b) \rangle$, then $G = \langle a \rangle$ and $H = \langle b \rangle$.

3. $\mathbb{Z}_2$ and $\mathbb{Z}_4$ are cyclic but $\mathbb{Z}_2 \times \mathbb{Z}_4$ is not.

4. $a^{mp} = e$ and $b^{nq} = e$ for any positive integers $p, q$. To find the order of $(a, b)$ we need to find the smallest $k$ such that $(a^k, b^k) = (e, e)$. So $k$ is the smallest integer such that $k = mp = nq$. In other words, $k = \text{lcm}(m, n)$.

5. $k = \text{lcm}(m, n) = \frac{mn}{\text{gcd}(m,n)} = mn$.

6. $\text{ord}(c, d) = \text{lcm}(m, n) = \frac{mn}{\text{gcd}(m,n)} < mn$ (because $\text{gcd}(m, n) > 1$).

7. (i) $\text{ord}(a)$ and $\text{ord}(b)$ are relatively prime. Then $\text{ord}(a, b) = mn$. So $(a, b)$ generates $G \times H$, since $|G \times H| = mn$.
   (ii) $G \times H$ is cyclic. Then $|G \times H| = mn$ and $\text{ord}(a) = m$ and $\text{ord}(b) = n$. So $m$ and $n$ are relatively prime.

## Chapter 15

### Set G

1. In the forward direction, for all $b \in G$, there is $x \in G$ such that:

$$\begin{aligned} a \sim b &\Rightarrow ax = xb \\ &\Rightarrow xa = xb \\ &\Rightarrow a = b \end{aligned} \tag{1}$$

   In the backward direction, consider the conjugacy class of $a$. It contains all elements of the form $xax^{-1}$. By the premise, the conjugacy class of $a$ contains only itself: $[a] = \{a\}$. So, for any $x \in G$, $a = xax^{-1}$ and, therefore, $ax = xa$. In other words, $a$ commutes with all elements of $G$ and, as such, $a \in C$.

2.

3.

4.

5.

6. Take any element $a \in G$. By Lagrange's Theorem, the order of $a$ is either $p$ or $p^2$. Let's consider each case separately:

   (a) (*There is an element with order $p^2$*) Since $|\langle a \rangle| = p^2 = |G|$, $\langle a \rangle = G$. So every element $x \in G$ can be uniquely written as $x = a^i$. The map $G \to \mathbb{Z}_{p^2}$ given by $x \mapsto a^i$, for $0 \leqslant i < p$, is an isomorphism.

   (b) (*There is no element with order $p^2$*) In this case all elements have order $p$. Consider the equivalence relation:

$$\begin{aligned} &e \sim e \\ &a \sim b \text{ iff } \langle a \rangle = \langle b \rangle \text{ and } a \neq e \text{ and } b \neq e \end{aligned}$$

   Take any $g, h \in G$ such that $g \nsim h$. Because equivalence relations define partitions, $\langle g \rangle \cap \langle h \rangle = \{e\}$, which means that $g^i \neq h^j$ for any $0 < i, j < p$. Now, consider that $g^i h^j = g^k h^l$ for some $0 \leqslant i, j, k, l < p$. Then $g^{i-k} = h^{l-j}$. The only way to satisfy this equation is making $i - k = 0$ and $l - j = 0$. So $i = k$ and $l = j$. Equivalently, $i \neq k$ or $l \neq j \Rightarrow g^i h^j \neq g^k h^l$. Also, there are $p^2$ different pairs $(i, j)$ such that $0 \leqslant i, j < p$. From these two facts, we can conclude that there are $p^2$ different products $g^i h^j$ and, therefore, any $x \in G$ can be uniquely written as $x = g^i h^j$ for some $0 \leqslant i, j < p$. So the map $G \to \mathbb{Z}_p \times \mathbb{Z}_p$, given by $g^i h^j \mapsto (i, j)$ is an isomorphism.

### Set H

1. ord$(a) = tp \Rightarrow (a^t)^p = e$. Assume that there is an integer $q < p$ such that $(a^t)^q = e$. Then $p$ is a multiple of $q$, which is a contradiction, since $p$ is prime. Therefore, ord$(a^t) = p$.

2. $k = pm$ for some integer $m$. Then $|G/\langle a\rangle| = |G|/|\langle a\rangle| = pm/$ ord$(a)$. Since ord$(a)$ is not a multiple of $p$, it must be a divisor of $m$. So $|G/\langle a\rangle| = p\frac{m}{\text{ord}(a)} < k$.

3. $G/\langle a\rangle$ is an abelian group and $|G/\langle a\rangle| < k$. Given that $p$ is a prime factor of $|G/\langle a\rangle|$, by the induction hypothesis $G/\langle a\rangle$ has an element of order $p$.

4. Let $c \in G/\langle a\rangle$. Then ord$(c) = p$ and ord$(c)m =$ ord$(a)$ for some positive integer $m$. Therefore, ord$(a) = pm \Rightarrow (a^m)^p = e \Rightarrow$ ord$(a^m) = p$.

## Chapter 16

### Set L

1. $C$ is a normal subgroup of $G$. So $|C| = mp$ for some positive integer $m$. By definition, $C$ is abelian. By 15.H, $C$ must contain at least one element of order $p$ (because $p$ is a prime factor of $mp$).

2. Being cyclic, $\langle a\rangle$ is a subgroup of $G$. Furthermore, $a$ is in the center of $G$. So, for all $x \in \langle a\rangle$ and all $g \in G$, $gx = xg$, which means that all elements $gxg^{-1}$ are in $\langle a\rangle$. Therefore $\langle a\rangle$ is a normal subgroup of $G$.

3. $|G/\langle a\rangle| = p^{k-1}$. Applying steps 1 and 2 again, we get another subgroup of order $p^{k-2}$ and so on down to order $p^1$.

### Set M

1. For all $g \in G$, ord$(g) = p^k$ for some positive integer $k$ and, thus, $|\langle g\rangle| = p^k$. By Cauchy's theorem, there is an $a \in \langle g\rangle$ such that ord$(a) = p$. And, because $p$ is prime, it is the only possible prime order that can exist for any element in $G$. Applying Cauchy's theorem now in reverse, since we have excluded all possible prime orders of elements, except $p$, the order of $G$ is a power of $p$ (by the fundamental theorem of arithmetic).