MA 407: Introduction to Modern Algebra
Homework Answers (Partial)

Hoon Hong

1 Group Theory

1.1 Definition of Group

1. State the definition of group.

   Let G be a set and let $\circ$ be a binary function from G. We say that $(G, \circ)$ is a group iff

   (a) "Closed": $\forall a, b \in G \quad a \circ b \in G$

   (b) "Associative": $\forall a, b, c \in G \quad (a \circ b) \circ c = a \circ (b \circ c)$

   (c) "Has Identity": $\exists e \in G \ \ \forall a \in G \quad a \circ e = e \circ a = a$

   (d) "Has Inverse" $\forall a \in G \ \ \exists b \in G \quad a \circ b = b \circ a = e$

   Actually, we need to combine "Has Identity" and "Has Inverse" into one statement as

   $$\exists e \in G \ [\forall a \in G \quad a \circ e = e \circ a = a] \ \wedge \ [\forall a \in G \ \ \exists b \in G \ a \circ b = b \circ a = e]$$

   so that they share the same "e". But for the sake of simple presentation, we split them into two separate conditions.

2. Is the following a group? If not, why not?

   (a) $(\{0, 1, 2\}, +)$
   False. Not closed: $1 + 2 = 3 \notin \{0, 1, 2\}$.

   (b) $(\{0, 1, 2\}, \circledcirc)$ where $a \circledcirc b$ is given by

$a \backslash b$	0	1	2
0	0	1	2
1	1	1	0
2	2	0	1

   False. Not associative: $(1 \circledcirc 1) \circledcirc 2 \neq 1 \circledcirc (1 \circledcirc 2)$

   (c) $(\mathbb{Z}^*, +)$ where $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$
   False. No identity.

   (d) $(\mathbb{Q}, \times)$
   False. The element $0 \in Q$ does not have an inverse.

1.2 Examples of Group

1. State the definition of the following notions:

   (a) $\mathbb{Z}_n, +_n$
   $\mathbb{Z}_n = \{0, \ldots, n-1\}$
   $a +_n b = \text{rem}\,(a+b, n)$

   (b) $U_n, \times_n$
   $U_n = \{k : 1 \le k \le n, \quad \gcd(k, n) = 1\}$
   $a \times_n b = \text{rem}\,(ab, n)$

   (c) $S_n, \circ$
   S_n is the set of all permutations of $\{1, \ldots, n\}$.
   $p \circ q : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ such that $(p \circ q)(x) = p(q(x))$.

   (d) $D_n, \circ$
   D_n is the set of all rigid motions that take a regular n-gon to itself.
   $p \circ q$: the motion q followed by the motion p.

2. Construct the operation tables.

   (a) $(\mathbb{Z}_4, \quad +_4)$

$a\backslash b$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

   (b) $(U_8, \quad \times_8)$

$a\backslash b$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

   (c) $(S_3, \quad \circ)$

$a\backslash b$	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_0	p_5	p_3	p_4
p_2	p_2	p_0	p_1	p_4	p_5	p_3
p_3	p_3	p_4	p_5	p_0	p_1	p_2
p_4	p_4	p_5	p_3	p_2	p_0	p_1
p_5	p_5	p_3	p_4	p_1	p_2	p_0

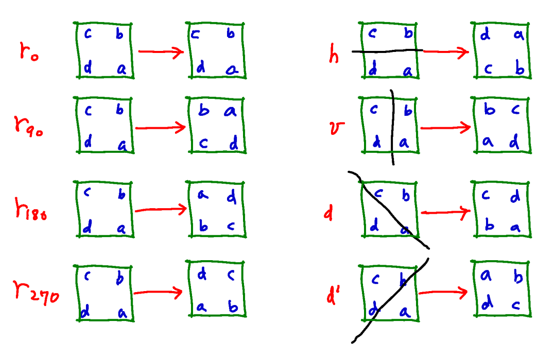
where

$$p_0 = \begin{bmatrix} 123 \\ 123 \end{bmatrix} \quad p_1 = \begin{bmatrix} 123 \\ 231 \end{bmatrix} \quad p_2 = \begin{bmatrix} 123 \\ 312 \end{bmatrix}$$

$$p_3 = \begin{bmatrix} 123 \\ 132 \end{bmatrix} \quad p_4 = \begin{bmatrix} 123 \\ 321 \end{bmatrix} \quad p_5 = \begin{bmatrix} 123 \\ 213 \end{bmatrix}$$

   (d) $(D_4, \quad \circ)$

$a\backslash b$	r_0	r_{90}	r_{180}	r_{270}	h	v	d	d'
r_0	r_0	r_{90}	r_{180}	r_{270}	h	v	d	d'
r_{90}	r_{90}	r_{180}	r_{270}	r_0	d'	d	h	v
r_{180}	r_{180}	r_{270}	r_0	r_{90}	v	h	d'	d
r_{270}	r_{270}	r_0	r_{90}	r_{180}	d	d'	v	h
h	h	d	v	d'	r_0	r_{180}	r_{90}	r_{270}
v	v	d'	h	d	r_{180}	r_0	r_{270}	r_{90}
d	d	v	d'	h	r_{270}	r_{90}	r_0	r_{180}
d'	d'	h	d	v	r_{90}	r_{270}	r_{180}	r_0



1.3 Uniqueness of Identity and Inverse

1. For each of the following groups, list identities and list inverses for each element

   (a) $(\mathbb{Z}_4, \ +_4)$

   - 0
   - $\begin{array}{c|cccc} a & 0 & 1 & 2 & 3 \\ a^{-1} & 0 & 3 & 2 & 1 \end{array}$

   (b) $(U_8, \ \times_8)$

   - 1
   - $\begin{array}{c|cccc} a & 1 & 3 & 5 & 7 \\ a^{-1} & 1 & 3 & 5 & 7 \end{array}$

   (c) $(S_3, \ \circ)$

   - p_0
   - $\begin{array}{c|cccccc} a & p_0 & p_1 & p_2 & p_3 & p_4 & p_5 \\ a^{-1} & p_0 & p_2 & p_1 & p_3 & p_4 & p_5 \end{array}$

   (d) $(D_4, \ \circ)$

   - r_0
   - $\begin{array}{c|cccccccc} a & r_0 & r_{90} & r_{180} & r_{270} & h & v & d & d' \\ a^{-1} & r_0 & r_{270} & r_{180} & r_{90} & h & v & d & d' \end{array}$

2. Prove: Let G be a group. Then G has only one identity element.

3. Prove: Let G be a group. Then every element of G has only one inverse.

1.4 Subgroup

1. State the definition of the following notions:

   (a) subgroup
   Let $(G, \circ)$ be a group. Then we say that S is a subgroup of G, and write $S \leq G$, iff
   (1) $S \subseteq G$.
   (2) $(S, \circ)$ is a group.

2. For each of the following groups, find all the subgroups.

   (a) $(\mathbb{Z}_4, \ \ +_4)$
   $\{0\}$
   $\{0, 2\}$
   $\{0, 1, 2, 3\}$

   (b) $(U_8, \ \times_8)$
   $\{1\}$
   $\{1, 3\}$
   $\{1, 5\}$
   $\{1, 7\}$
   $\{1, 3, 5, 7\}$

   (c) $(S_3, \ \ \circ)$
   $\{p_0\}$
   $\{p_0, p_3\}$
   $\{p_0, p_4\}$
   $\{p_0, p_5\}$
   $\{p_0, p_1, p_2\}$
   $\{p_0, p_1, p_2, p_3, p_4, p_5\}$

   (d) $(D_4, \ \circ)$
   $\{r_0\}$
   $\{r_0, r_{180}\}$
   $\{r_0, h\}$
   $\{r_0, v\}$
   $\{r_0, d\}$
   $\{r_0, d'\}$
   $\{r_0, r_{90}, r_{180}, r_{270}\}$
   $\{r_0, r_{180}, h, v\}$
   $\{r_0, r_{180}, d, d'\}$
   $\{r_0, r_{90}, r_{180}, r_{270}, h, v, d, d'\}$

3. Prove: Let G be a group and $S \subseteq G$. We have $S \leq G$ iff

   (a) $S \neq \emptyset$
   (b) $\forall a, b \in S \ \ ab^{-1} \in S$.

1.5 Normal subgroup and Quotient group

1. State the definition of the following notions

   (a) normal subgroup
   Let G be a group and let $S \leq G$. Then we say that S is a normal subgroup of G, and write $S \lhd G$, iff

   $$\forall a \in G \;\; aS = Sa$$

   (b) quotient set
   Let G be a group and let $S \lhd G$. Then the quotient set, written as G/S, is defined by

   $$G/S = \{aS : a \in G\}$$

   (c) operation over G/S.
   Let G be a group and let $S \lhd G$. Let $aS, bS \in G/S$. Then

   $$(aS)(bS) = (ab)S$$

2. For each of the following groups G

   (a) $(\mathbb{Z}_4, \;\; +_4)$

   - Find all the normal subgroups of G.
     $S = \{0\}$
     $0S = \{0\} = S0$
     $1S = \{1\} = S1$
     $2S = \{2\} = S2$
     $3S = \{3\} = S3$
     $S = \{0, 2\}$
     $0S = 2S = \{0, 2\} = S0 = S2$
     $1S = 3S = \{1, 3\} = S1 = S3$
     $S = \mathbb{Z}_4$
     $0S = 1S = 2S = 3S = \mathbb{Z}_4 = S0 = S1 = S2 = S3$
   - For each normal subgroup S, construct the operation table on G/S.
     $S = \{0\}$

$a \backslash b$	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$
$\{0\}$	$\{0\}$	$\{1\}$	$\{2\}$	$\{3\}$
$\{1\}$	$\{1\}$	$\{2\}$	$\{3\}$	$\{0\}$
$\{2\}$	$\{2\}$	$\{3\}$	$\{0\}$	$\{1\}$
$\{3\}$	$\{3\}$	$\{0\}$	$\{1\}$	$\{2\}$

     $S = \{0, 2\}$

$a \backslash b$	$\{0, 2\}$	$\{1, 3\}$
$\{0, 2\}$	$\{0, 2\}$	$\{1, 3\}$
$\{1, 3\}$	$\{1, 3\}$	$\{0, 2\}$

     $S = \mathbb{Z}_4$

$a \backslash b$	$\mathbb{Z}_4$
$\mathbb{Z}_4$	$\mathbb{Z}_4$

   - Check if G/S is a group.
     Obvious from the tables.

(b) $(U_8, \times_8)$

- Find all the normal subgroups of G.

  $S = \{1\}$

  $1S = \{1\} = S1$
  $3S = \{3\} = S3$
  $5S = \{5\} = S5$
  $7S = \{7\} = S7$

  $S = \{1, 3\}$
  $1S = 3S = \{1, 3\} = S1 = S3$
  $5S = 7S = \{5, 7\} = S5 = S7$

  $S = \{1, 5\}$
  $1S = 5S = \{1, 5\} = S1 = S5$
  $3S = 7S = \{3, 7\} = S3 = S7$

  $S = \{1, 7\}$
  $1S = 7S = \{1, 7\} = S1 = S7$
  $3S = 5S = \{3, 5\} = S3 = S5$

  $S = U_8$
  $1S = 3S = 5S = 7S = U_8 = S1 = S3 = S5 = S7$

- For each normal subgroup S, construct the operation table on G/S.

  $S = \{1\}$

$a\backslash b$	$\{1\}$	$\{3\}$	$\{5\}$	$\{7\}$
$\{1\}$	$\{1\}$	$\{3\}$	$\{5\}$	$\{7\}$
$\{3\}$	$\{3\}$	$\{1\}$	$\{7\}$	$\{5\}$
$\{5\}$	$\{5\}$	$\{7\}$	$\{1\}$	$\{3\}$
$\{7\}$	$\{7\}$	$\{5\}$	$\{3\}$	$\{1\}$

  $S = \{1, 3\}$

$a\backslash b$	$\{1, 3\}$	$\{5, 7\}$
$\{1, 3\}$	$\{1, 3\}$	$\{5, 7\}$
$\{5, 7\}$	$\{5, 7\}$	$\{1, 3\}$

  $S = \{1, 5\}$

$a\backslash b$	$\{1, 5\}$	$\{3, 7\}$
$\{1, 5\}$	$\{1, 5\}$	$\{3, 7\}$
$\{3, 7\}$	$\{3, 7\}$	$\{1, 5\}$

  $S = \{1, 7\}$

$a\backslash b$	$\{1, 7\}$	$\{3, 5\}$
$\{1, 7\}$	$\{1, 7\}$	$\{3, 5\}$
$\{3, 5\}$	$\{3, 5\}$	$\{1, 7\}$

  $S = U_8$

$a\backslash b$	U_8
U_8	U_8

- Check if G/S is a group.
  Obvious from the tables.

(c) $(S_3, \ \circ)$

- Find all the normal subgroups of G.

  $S = \{p_0\}$

  $p_0S = \{p_0\} = Sp_0$
  $p_1S = \{p_1\} = Sp_1$
  $p_2S = \{p_2\} = Sp_2$
  $p_3S = \{p_3\} = Sp_3$
  $p_4S = \{p_4\} = Sp_4$
  $p_5S = \{p_5\} = Sp_5$

  $S = \{p_0, p_1, p_2\}$

  $p_0S = p_1S = p_2S = \{p_0, p_1, p_2\} = Sp_0 = Sp_1 = Sp_2$
  $p_3S = p_4S = p_5S = \{p_3, p_4, p_5\} = Sp_3 = Sp_4 = Sp_5$

  $S = S_3$

  $p_0S = p_1S = p_2S = p_3S = p_4S = p_5S = S_3 = Sp_0 = Sp_1 = Sp_2 = Sp_3 = Sp_4 = Sp_5$

- For each normal subgroup S, construct the operation table on G/S.

  $S = \{p_0\}$

$a \backslash b$	$\{p_0\}$	$\{p_1\}$	$\{p_2\}$	$\{p_3\}$	$\{p_4\}$	$\{p_5\}$
$\{p_0\}$	$\{p_0\}$	$\{p_1\}$	$\{p_2\}$	$\{p_3\}$	$\{p_4\}$	$\{p_5\}$
$\{p_1\}$	$\{p_1\}$	$\{p_2\}$	$\{p_0\}$	$\{p_5\}$	$\{p_3\}$	$\{p_4\}$
$\{p_2\}$	$\{p_2\}$	$\{p_0\}$	$\{p_1\}$	$\{p_4\}$	$\{p_5\}$	$\{p_3\}$
$\{p_3\}$	$\{p_3\}$	$\{p_4\}$	$\{p_5\}$	$\{p_0\}$	$\{p_1\}$	$\{p_2\}$
$\{p_4\}$	$\{p_4\}$	$\{p_5\}$	$\{p_3\}$	$\{p_2\}$	$\{p_0\}$	$\{p_1\}$
$\{p_5\}$	$\{p_5\}$	$\{p_3\}$	$\{p_4\}$	$\{p_1\}$	$\{p_2\}$	$\{p_0\}$

  $S = \{p_0, p_1, p_2\}$

$a \backslash b$	$\{p_0, p_1, p_2\}$	$\{p_3, p_4, p_5\}$
$\{p_0, p_1, p_2\}$	$\{p_0, p_1, p_2\}$	$\{p_3, p_4, p_5\}$
$\{p_3, p_4, p_5\}$	$\{p_3, p_4, p_5\}$	$\{p_0, p_1, p_2\}$

  $S = S_3$

$a \backslash b$	S_3
S_3	S_3

- Check if G/S is a group.
  Obvious from the tables.

(d) $(D_4, \circ)$

- Find all the normal subgroups of G.
  $S = \{r_0\}$
  $r_0 S = \{r_0\} = S r_0$
  $r_{90} S = \{r_{90}\} = S r_{90}$
  $r_{180} S = \{r_{180}\} = S r_{180}$
  $r_{270} S = \{r_{270}\} = S r_{270}$
  $hS = \{h\} = Sh$
  $vS = \{v\} = Sv$
  $dS = \{d\} = Sd$
  $d'S = \{d'\} = Sd'$
  $S = \{\{r_0, r_{180}\}\}$
  $r_0 S = r_{180} S = \{r_0, r_{180}\} = S r_0 = S r_{180}$
  $r_{90} S = r_{270} S = \{r_{90}, r_{270}\} = S r_{90} = S r_{270}$
  $hS = vS = \{h, v\} = Sh = Sv$
  $dS = d'S = \{d, d'\} = Sd = Sd'$
  $S = \{r_0, r_{90}, r_{180,} r_{270}\}$
  $r_0 S = r_{90} S = r_{180} S = r_{270} S = \{r_0, r_{90}, r_{180}, r_{270}\} = S r_0 = S r_{90} = S r_{180} = S r_{270}$
  $hS = dS = vS = d'S = \{h, d, v, d'\} = Sh = Sv = Sd = Sd'$
  $S = \{r_0, r_{180,} h, v\}$
  $r_0 S = r_{180} S = hS = vS = \{r_0, r_{180}, h, v\} = S r_0 = S r_{180} = Sh = Sv$
  $r_{90} S = r_{270} S = d'S = dS = \{r_{90}, r_{270}, d', d\} = S r_{90} = S r_{270} = Sd = Sd'$
  $S = \{r_0, r_{180,} d, d'\}$
  $r_0 S = r_{180} S = dS = d'S = \{r_0, r_{180}, d, d'\} = S r_0 = S r_{180} = Sd = Sd'$
  $r_{90} S = r_{270} S = hS = vS = \{r_{90}, r_{270}, h, v\} = S r_{90} = S r_{270} = Sh = Sv$
  $S = D_4$
  $r_0 S = r_{90} S = r_{180} S = r_{270} S = hS = vS = dS = d'S = D_4 =$
  $S r_0 = S r_{90} = S r_{180} = S r_{270} = Sh = Sv = Sd = Sd'$
- For each normal subgroup S, construct the operation table on G/S.
  $S = \{r_0\}$

$a \backslash b$	$\{r_0\}$	$\{r_{90}\}$	$\{r_{180}\}$	$\{r_{270}\}$	$\{h\}$	$\{v\}$	$\{d\}$	$\{d'\}$
$\{r_0\}$	$\{r_0\}$	$\{r_{90}\}$	$\{r_{180}\}$	$\{r_{270}\}$	$\{h\}$	$\{v\}$	$\{d\}$	$\{d'\}$
$\{r_{90}\}$	$\{r_{90}\}$	$\{r_{180}\}$	$\{r_{270}\}$	$\{r_0\}$	$\{d'\}$	$\{d\}$	$\{h\}$	$\{v\}$
$\{r_{180}\}$	$\{r_{180}\}$	$\{r_{270}\}$	$\{r_0\}$	$\{r_{90}\}$	$\{v\}$	$\{h\}$	$\{d'\}$	$\{d\}$
$\{r_{270}\}$	$\{r_{270}\}$	$\{r_0\}$	$\{r_{90}\}$	$\{r_{180}\}$	$\{d\}$	$\{d'\}$	$\{v\}$	$\{h\}$
$\{h\}$	$\{h\}$	$\{d\}$	$\{v\}$	$\{d'\}$	$\{r_0\}$	$\{r_{180}\}$	$\{r_{90}\}$	$\{r_{270}\}$
$\{v\}$	$\{v\}$	$\{d'\}$	$\{h\}$	$\{d\}$	$\{r_{180}\}$	$\{r_0\}$	$\{r_{270}\}$	$\{r_{90}\}$
$\{d\}$	$\{d\}$	$\{v\}$	$\{d'\}$	$\{h\}$	$\{r_{270}\}$	$\{r_{90}\}$	$\{r_0\}$	$\{r_{180}\}$
$\{d'\}$	$\{d'\}$	$\{h\}$	$\{d\}$	$\{v\}$	$\{r_{90}\}$	$\{r_{270}\}$	$\{r_{180}\}$	$\{r_0\}$

  $S = \{\{r_0, r_{180}\}\}$

$a \backslash b$	$\{r_0, r_{180}\}$	$\{r_{90}, r_{270}\}$	$\{h, v\}$	$\{d, d'\}$
$\{r_0, r_{180}\}$	$\{r_0, r_{180}\}$	$\{r_{90}, r_{270}\}$	$\{h, v\}$	$\{d, d'\}$
$\{r_{90}, r_{270}\}$	$\{r_{90}, r_{270}\}$	$\{r_0, r_{180}\}$	$\{d, d'\}$	$\{h, v\}$
$\{h, v\}$	$\{h, v\}$	$\{d, d'\}$	$\{r_0, r_{180}\}$	$\{r_{90}, r_{270}\}$
$\{d, d'\}$	$\{d, d'\}$	$\{h, v\}$	$\{r_{90}, r_{270}\}$	$\{r_0, r_{180}\}$

  $S = \{r_0, r_{90}, r_{180,} r_{270}\}$

$a \backslash b$	$\{r_0, r_{90}, r_{180}, r_{270}\}$	$\{h, v, d, d'\}$
$\{r_0, r_{90}, r_{180}, r_{270}\}$	$\{r_0, r_{90}, r_{180}, r_{270}\}$	$\{h, v, d, d'\}$
$\{h, v, d, d'\}$	$\{h, v, d, d'\}$	$\{r_0, r_{90}, r_{180}, r_{270}\}$

$S=\{r_0,r_{180},h,v\}$

$a\backslash b$	$\{r_0,r_{180},h,v\}$	$\{r_{90},r_{270},d,d'\}$
$\{r_0,r_{180},h,v\}$	$\{r_0,r_{180},h,v\}$	$\{r_{90},r_{270},d,d'\}$
$\{r_{90},r_{270},d,d'\}$	$\{r_{90},r_{270},d,d'\}$	$\{r_0,r_{180},h,v\}$

$S=\{r_0,r_{180},d,d'\}$

$a\backslash b$	$\{r_0,r_{180},d,d'\}$	$\{r_{90},r_{270},h,v\}$
$\{r_0,r_{180},d,d'\}$	$\{r_0,r_{180},d,d'\}$	$\{r_{90},r_{270},h,v\}$
$\{r_{90},r_{270},h,v\}$	$\{r_{90},r_{270},h,v\}$	$\{r_0,r_{180},d,d'\}$

$S=D_4$

$a\backslash b$	D_4
D_4	D_4

- Check if G/S is a group.
  Obvious from the tables.

3. Prove: Let G be a group and let $S \lhd G$. Then the operation over G/S is well defined, that is, if $aS=a'S$ and $bS=b'S$ then $(ab)\,S=(a'b')\,S$.

4. Prove: Let G be a group and let $S \lhd G$. Then G/S is a group.

1.6 Homomorphism, Isomorphism, Image and Kernel

1. State the definition of the following notions.

   Let $(G, \circ), (G', \circ')$ be groups. Let $\phi : G \longrightarrow G'$.

   (a) Homomorphism

   ϕ is called a homomorphism iff $\forall a, b \in G \;\; \phi(a \circ b) = \phi(a) \circ' \phi(b)$.

   (b) Isomorphism

   ϕ is called an isomorphism iff it is homomorphism, one-to-one and onto.

   (c) Isomorphic ($\cong$)

   $G \cong G'$ iff there is an isomorphism $\phi : G \longrightarrow G'$.

   (d) Kernel

   $\ker\phi = \{a \in G : \phi(a) = e'\}$.

   (e) Image

   $\operatorname{im}\phi = \{\phi(a) : a \in G\}$.

2. For each of the following maps $\phi : (G, \circ) \longrightarrow (G', \circ')$ do

   (a) $\phi : (\mathbb{Z}_9, +_9) \longrightarrow (\mathbb{Z}_9, +_9)$, given by $x \longmapsto 3 \times_9 x$

   - Draw the map diagram for ϕ.

     $$\begin{array}{ccc} 0 & \mapsto & 0 \\ 1 & \mapsto & 3 \\ 2 & \mapsto & 6 \\ 3 & \mapsto & 0 \\ 4 & \mapsto & 3 \\ 5 & \mapsto & 6 \\ 6 & \mapsto & 0 \\ 7 & \mapsto & 3 \\ 8 & \mapsto & 6 \end{array}$$

   - Verify that ϕ is a homomorphism.

     Obvious from the diagram.

   - Construct the operation table for $\operatorname{im}\phi$, and verify that $\operatorname{im}\phi \leq G'$.

$a \backslash b$	0	3	6
0	0	3	6
3	3	6	0
6	6	0	3

     Obvious from the table that $\operatorname{im}\phi \leq \mathbb{Z}_9$.

   - Construct the operation table for $\ker\phi$, and verify that $\ker\phi \lhd G$.

$a \backslash b$	0	3	6
0	0	3	6
3	3	6	0
6	6	0	3

     Obvious from the table that $\ker\phi \lhd \mathbb{Z}_9$.

   - Construct the operation table for $G/\ker\phi$.

$a \backslash b$	$\{0,3,6\}$	$\{1,4,7\}$	$\{2,5,8\}$
$\{0,3,6\}$	$\{0,3,6\}$	$\{1,4,7\}$	$\{2,5,8\}$
$\{1,4,7\}$	$\{1,4,7\}$	$\{2,5,8\}$	$\{0,3,6\}$
$\{2,5,8\}$	$\{2,5,8\}$	$\{0,3,6\}$	$\{1,4,7\}$

- Draw the map diagram for the "natural" isomorphism that shows $G/\ker\phi \cong \operatorname{im}\phi$.

$$\begin{array}{lcl} \{0,3,6\} & \mapsto & 0 \\ \{1,4,7\} & \mapsto & 3 \\ \{2,5,8\} & \mapsto & 6 \end{array}$$

(b) $\phi : (U_8, \times_8) \longrightarrow (U_8, \times_8)$, given by $x \longmapsto \begin{cases} 1 & \text{if } x \text{ is 1 or 3} \\ 5 & \text{otherwise} \end{cases}$

- Draw the map diagram for ϕ.

$$\begin{array}{lcl} 1 & \mapsto & 1 \\ 3 & \mapsto & 1 \\ 5 & \mapsto & 5 \\ 7 & \mapsto & 5 \end{array}$$

- Verify that ϕ is a homomorphism.
Obvious from the diagram.
- Construct the operation table for $\operatorname{im}\phi$, and verify that $\operatorname{im}\phi \le G'$.

$a\backslash b$	1	5
1	1	5
5	5	1

Obvious from the table that $\operatorname{im}\phi \le U_8$.
- Construct the operation table for $\ker\phi$, and verify that $\ker\phi \lhd G$.

$a\backslash b$	1	3
1	1	3
3	3	1

Obvious from the table that $\ker\phi \lhd U_8$.
- Construct the operation table for $G/\ker\phi$.

$a\backslash b$	$\{1,3\}$	$\{5,7\}$
$\{1,3\}$	$\{1,3\}$	$\{5,7\}$
$\{5,7\}$	$\{5,7\}$	$\{1,3\}$

- Draw the map diagram for the "natural" isomorphism that shows $G/\ker\phi \cong \operatorname{im}\phi$.

$$\begin{array}{lcl} \{1,3\} & \mapsto & 1 \\ \{5,7\} & \mapsto & 5 \end{array}$$

(c) $\phi : (S_3, \circ) \longrightarrow (U_8, \times_8)$, given by $x \longmapsto \begin{cases} 1 & \text{if } x \text{ is an even permutation} \\ 3 & \text{otherwise} \end{cases}$.

- Draw the map diagram for ϕ.

$$\begin{array}{lcl} p_0 & \mapsto & 1 \\ p_1 & \mapsto & 1 \\ p_2 & \mapsto & 1 \\ p_3 & \mapsto & 3 \\ p_4 & \mapsto & 3 \\ p_5 & \mapsto & 3 \end{array}$$

- Verify that ϕ is a homomorphism.
Obvious from the diagram.
- Construct the operation table for $\operatorname{im}\phi$, and verify that $\operatorname{im}\phi \le G'$.

$a\backslash b$	1	3
1	1	3
3	3	1

Obvious from the table that $\operatorname{im}\phi \le U_8$.
- Construct the operation table for $\ker\phi$, and verify that $\ker\phi \lhd G$.

$a\backslash b$	p_0	p_1	p_2
p_0	p_0	p_1	p_2
p_1	p_1	p_2	p_0
p_2	p_2	p_0	p_1

Obvious from the table that $\ker\phi \lhd\ S_3$.

- Construct the operation table for $G/\ker\phi$.

$a\backslash b$	$\{p_0, p_1, p_2\}$	$\{p_3, p_4, p_5\}$
$\{p_0, p_1, p_2\}$	$\{p_0, p_1, p_2\}$	$\{p_3, p_4, p_5\}$
$\{p_3, p_4, p_5\}$	$\{p_3, p_4, p_5\}$	$\{p_0, p_1, p_2\}$

- Draw the map diagram for the "natural" isomorphism that shows $G/\ker\phi \cong \operatorname{im}\phi$.

$$\begin{array}{ccc} \{p_0, p_1, p_2\} & \mapsto & 1 \\ \{p_3, p_4, p_5\} & \mapsto & 3 \end{array}$$

(d) $\phi : (D_4,\ \circ) \longrightarrow (\mathbb{Z}_4,\ +_4)$, given by $x \longmapsto \begin{cases} 0 & \text{if } x \text{ is a rotation} \\ 2 & \text{otherwise} \end{cases}$

- Draw the map diagram for ϕ.

$$\begin{array}{ccc} r_0 & \mapsto & 0 \\ r_{90} & \mapsto & 0 \\ r_{180} & \mapsto & 0 \\ r_{270} & \mapsto & 0 \\ h & \mapsto & 2 \\ v & \mapsto & 2 \\ d & \mapsto & 2 \\ d' & \mapsto & 2 \end{array}$$

- Verify that ϕ is a homomorphism.
  Obvious from the diagram.
- Construct the operation table for $\operatorname{im}\phi$, and verify that $\operatorname{im}\phi\ \leq G'$.

$a\backslash b$	0	2
0	0	2
2	2	0

Obvious from the table that $\operatorname{im}\phi\ \leq \mathbb{Z}_4$.

- Construct the operation table for $\ker\phi$, and verify that $\ker\phi \lhd\ G$.

$a\backslash b$	r_0	r_{90}	r_{180}	r_{270}
r_0	r_0	r_{90}	r_{180}	r_{270}
r_{90}	r_{90}	r_{180}	r_{270}	r_0
r_{180}	r_{180}	r_{270}	r_0	r_{90}
r_{270}	r_{270}	r_0	r_{90}	r_{180}

Obvious from the table that $\ker\phi \lhd\ D_4$.

- Construct the operation table for $G/\ker\phi$.

$a\backslash b$	$\{r_0, r_{90}, r_{180}, r_{270}\}$	$\{h, v, d, d'\}$
$\{r_0, r_{90}, r_{180}, r_{270}\}$	$\{r_0, r_{90}, r_{180}, r_{270}\}$	$\{h, v, d, d'\}$
$\{h, v, d, d'\}$	$\{h, v, d, d'\}$	$\{r_0, r_{90}, r_{180}, r_{270}\}$

- Draw the map diagram for the "natural" isomorphism that shows $G/\ker\phi \cong \operatorname{im}\phi$.

$$\begin{array}{ccc} \{r_0, r_{90}, r_{180}, r_{270}\} & \mapsto & 0 \\ \{h, v, d, d'\} & \mapsto & 2 \end{array}$$

3. Prove: Let $\phi : (G, \circ) \longrightarrow (G', \circ')$ be a homomorphism. Then $\phi(e) = e'$.

4. Prove: Let $\phi : (G, \circ) \longrightarrow (G', \circ')$ be a homomorphism. Then $\forall a \in G \;\; \phi\left(a^{-1}\right) = \phi(a)^{-1'}$.

5. Prove: Let $\phi : (G, \circ) \longrightarrow (G', \circ')$ be a homomorphism. Then $\operatorname{im}\phi \;\leq\; G'$.

6. Prove: Let $\phi : (G, \circ) \longrightarrow (G', \circ')$ be a homomorphism. Then $\ker\phi \leq\; G$.

7. Prove: Let $\phi : (G, \circ) \longrightarrow (G', \circ')$ be a homomorphism. Then $\ker\phi \lhd\; G$.

8. Prove: Let $\phi : (G, \circ) \longrightarrow (G', \circ')$ be a homomorphism. Then $G/\ker\phi \cong \operatorname{im}\phi$.

2 Ring Theory

2.1 Definition of Ring

1. State the definitions of the following abstract notions

   (a) Ring
   We say that $(R, +, \cdot)$ is a ring iff
   (A) $+$
      1. Closed: $\forall a, b \in R \;\; a + b \in R$
      2. Associative: $\forall a, b, c \in R \;\; (a + b) + c = a + (b + c)$
      3. Commutative: $\forall a, b \in R \; a + b = b + a$
      4. Has identity: $\exists 0 \in R \; \forall a \in R \;\; a + 0 = a$
      5. Has inverse: $\forall a \in R \; \exists b \in R \; a + b = 0$

   (B) $\cdot$
      1. Closed: $\forall a, b \in R \;\; a \cdot b \in R$
      2. Associative: $\forall a, b, c \in R \;\; (a \cdot b) \cdot c = a \cdot (b \cdot c)$

   (C) $+, \cdot$
      1. Distributive: $\forall a, b, c \in R \;\; (a + b) \cdot c = (a \cdot c) + (b \cdot c)$ and $a \cdot (b + c) = a \cdot b + a \cdot c$

   (b) Commutative Ring
   We say that $(R, +, \cdot)$ is a commutative ring iff
   - it is a ring
   - $\cdot$ is commutative: $\forall a, b \in R \; a \cdot b = b \cdot a$

   (c) Ring with Unity
   We say that $(R, +, \cdot)$ is a ring with unity iff
   - it is a ring
   - $\cdot$ has an identity: $\exists 1 \in R \; \forall a \in R \;\; a \cdot 1 = 1 \cdot a = a$

   (d) Commutative Ring with Unity (CRU)
   We say that $(R, +, \cdot)$ is a commutative ring with unity iff
   - it is a ring
   - $\cdot$ is commutative
   - $\cdot$ has identity.

   (e) Integral domain
   We say that $(R, +, \cdot)$ is an integral domain iff
   - it is a CRU.
   - it does not have a zero-divisor: $\nexists a, b \in R \backslash \{0\} \quad a \cdot b = 0$.

   (f) Field
   We say that $(R, +, \cdot)$ is a field iff
   - it is a CRU
   - $\cdot$ has inverse for non-zero element (the identity for $+$): $\forall a \in R \backslash \{0\} \; \exists b \in R \; a \cdot b = 1$

2.2 Examples of Ring

1. State the definitions of the following concrete notations.

   (a) $k\mathbb{Z} = \{ka : a \in \mathbb{Z}\}$

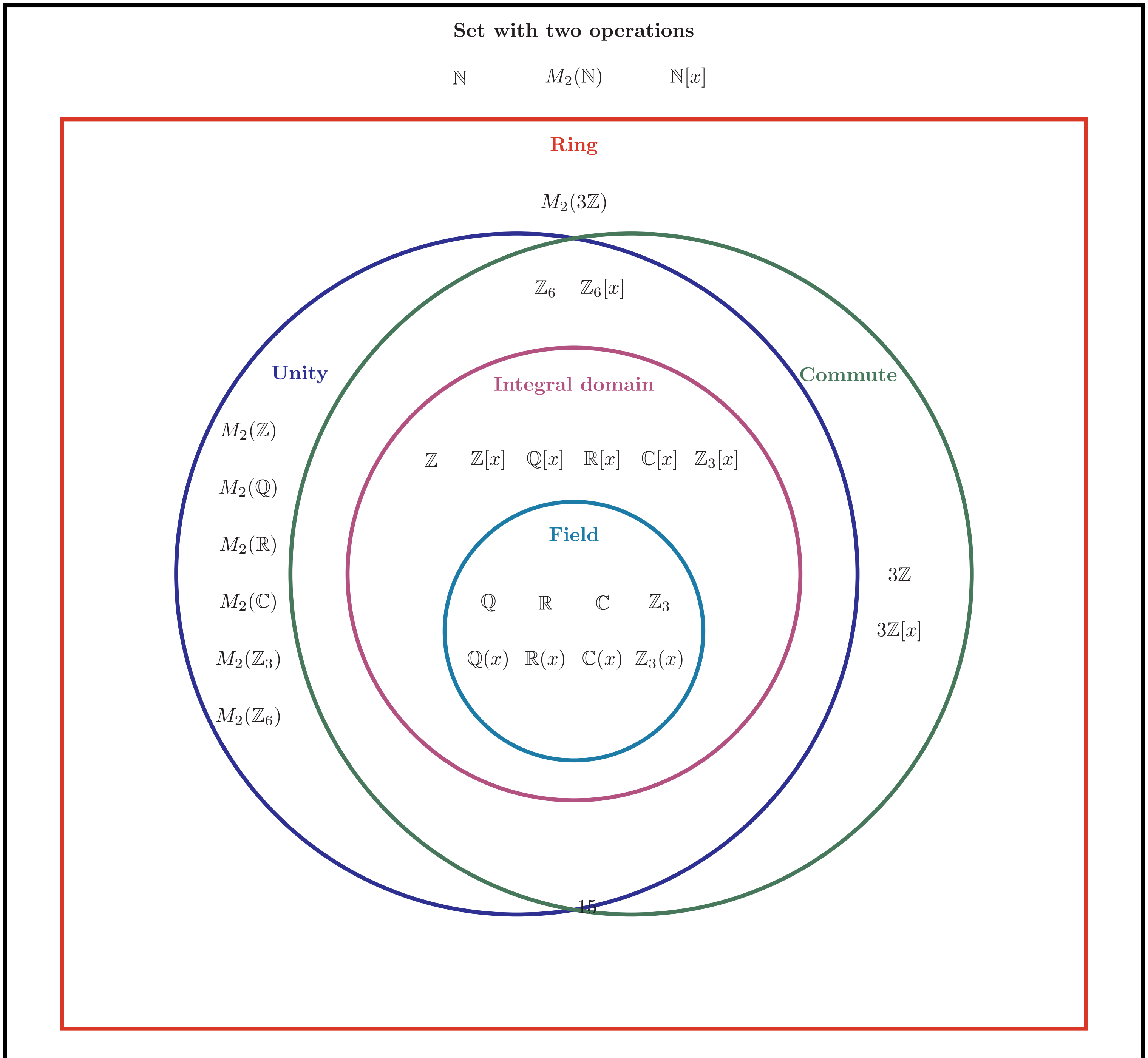
   (b) $M_n(S) =$ the set of all n by n matrices with the entries from the set S.

   (c) $S[x] =$ the set of all polynomials in the variable x with the coefficients from the set S.

   (d) $S(x) =$ the set of all rational functions in the variable x with the coefficients from the set S.

2. Classify the following algebraic structures, using a Venn diagram (as we have done in the class).

$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{Z}_3$	$\mathbb{Z}_6$	$3\mathbb{Z}$
$M_2(\mathbb{N})$	$M_2(\mathbb{Z})$	$M_2(\mathbb{Q})$	$M_2(\mathbb{R})$	$M_2(\mathbb{C})$	$M_2(\mathbb{Z}_3)$	$M_2(\mathbb{Z}_6)$	$M_2(3\mathbb{Z})$
$\mathbb{N}[x]$	$\mathbb{Z}[x]$	$\mathbb{Q}[x]$	$\mathbb{R}[x]$	$\mathbb{C}[x]$	$\mathbb{Z}_3[x]$	$\mathbb{Z}_6[x]$	$3\mathbb{Z}[x]$
		$\mathbb{Q}(x)$	$\mathbb{R}(x)$	$\mathbb{C}(x)$	$\mathbb{Z}_3(x)$		



2.3 Uniqueness of identity and inverse

1. Prove: Let R be a ring. Then there is only one additive identity.

2. Prove: Let R be a ring. Then every element of R has has only one additive inverse.

3. Prove: Let R be a ring with unity. Then there is only one multiplicative identity.

4. Prove: Let R be a field. Then every non-zero element of R has only one multiplicative inverse.

2.4 Subring

1. State the definitions of the following notions:

   (a) Subring
   Let $(R, +, \cdot)$ be a ring. Then we say that S is a subring of R, and write $S \leq R$, iff
   (1) $S \subseteq R$.
   (2) $(S, +, \cdot)$ is a ring.

2. Check the truth of the followings.

   (a) $3\mathbb{Z} \leq \mathbb{Z}$
   True.
   (b) $\{0, 5\} \leq \mathbb{Z}_{12}$
   False. Not closed under $+_{12}$.
   (c) $2\mathbb{Z}_{12} \leq \mathbb{Z}_{12}$
   True.
   (d) $3\mathbb{Z}_{12} \leq \mathbb{Z}_{12}$
   True.
   (e) $4\mathbb{Z}_{12} \leq \mathbb{Z}_{12}$
   True.
   (f) $6\mathbb{Z}_{12} \leq \mathbb{Z}_{12}$
   True.
   (g) $\{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\} \leq \mathbb{C}$
   True
   (h) $\left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\} \leq M_2(\mathbb{R})$
   True

3. Prove: Let R be a ring and $S \subseteq R$. We have $S \leq R$ if

   (a) $S \neq \emptyset$
   (b) $\forall a, b \in S \;\; a + (-b) \in S$
   (c) $\forall a, b \in S \;\; a \cdot b \in S$

2.5 Ideal and Quotient ring

1. State the definitions of the following notions:

   (a) Ideal
   Let R be a ring and let $I \leq R$.
   We say that I is an ideal of R, and write $I \lhd R$, iff $\forall a \in I\ \forall b \in R \quad ab, ba \in I$.

   (b) Generated set
   Let R be a CRU and let $a_1, \ldots, a_n \in R$. Then the set generated by $a_1, \ldots, a_n$, written as $\langle a_1, \ldots, a_n \rangle$, is defined by

   $$\langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_1, \ldots, r_n \in R\}$$

   (c) Quotient set
   Let R be a ring and let $I \lhd R$. The quotient set of R mod I, written as R/I, is defined by

   $$R/I = \{r + I : r \in R\}$$

   (d) Operation on quotient set
   Let R be a ring and let $I \lhd R$. Let $a + I, b + I \in R/I$. We define

   $$(a + I) + (b + I) = (a + b) + I$$
   $$(a + I) \cdot (b + I) = (a \cdot b) + I$$

2. Check the truth of the followings.

   (a) $3\mathbb{Z} \lhd \mathbb{Z}$
   True.

   (b) $\{0, 5\} \lhd \mathbb{Z}_{12}$
   False. Not closed under $+_{12}$.

   (c) $2\mathbb{Z}_{12} \lhd \mathbb{Z}_{12}$
   True.

   (d) $3\mathbb{Z}_{12} \lhd \mathbb{Z}_{12}$
   True.

   (e) $4\mathbb{Z}_{12} \lhd \mathbb{Z}_{12}$
   True.

   (f) $6\mathbb{Z}_{12} \lhd \mathbb{Z}_{12}$
   True.

   (g) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \lhd \mathbb{C}$
   False. Note $\frac{1}{2} \cdot (1 + 0i) \notin \mathbb{Z}[i]$

   (h) $\left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\} \lhd M_2(\mathbb{R})$
   False. Note $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

3. List the elements of the following sets:

   (a) $\langle 3 \rangle$ as an ideal of $\mathbb{Z}$
   $\{\ldots, -6, -3, 0, 3, 6, ...\}$

(b) $\langle 8, 12\rangle$ as an ideal of $\mathbb{Z}$
$\{\ldots, -8, -4, 0, 4, 8, \ldots\}$

(c) $\langle 2\rangle$ as an ideal of $\mathbb{Z}_8$
$\{0, 2, 4, 6\}$

(d) $\langle 4\rangle$ as an ideal of $\mathbb{Z}_8$
$\{0, 4\}$

(e) $\langle x\rangle$ as an ideal of $\mathbb{Z}_2[x]$
$\left\{0, x,\ \ x^2, x^2+x^1,\ \ x^3, x^3+x^1, x^3+x^2, x^3+x^2+x^1,\ \ldots\right\}$

(f) $\langle x^2\rangle$ as an ideal of $\mathbb{Z}_2[x]$
$\left\{0, x^2,\ \ x^3, x^3+x^2,\ \ x^4, x^4+x^2, x^4+x^3, x^4+x^3+x^2, \ldots\right\}$

4. For each of the following structures

(a) $\mathbb{Z}/\langle 3\rangle$

- List the elements.
  $\{c_0, c_1, c_2\}$ where
  $c_0 = 0 + \langle 3\rangle = \{\ldots, -6, -3, 0, 3, 6, ...\}$
  $c_1 = 1 + \langle 3\rangle = \{\ldots, -5, -2, 1, 4, 7, ...\}$
  $c_2 = 2 + \langle 3\rangle = \{\ldots, -4, -1, 2, 5, 8, ...\}$
- Construct the operation tables for addition and multiplication

$+$	c_0	c_1	c_2	$\cdot$	c_0	c_1	c_2
c_0	c_0	c_1	c_2	c_0	c_0	c_0	c_0
c_1	c_1	c_2	c_0	c_1	c_0	c_1	c_2
c_2	c_2	c_0	c_1	c_2	c_0	c_2	c_1

- Verify that it is a ring.
  Obvious from the tables.

(b) $\mathbb{Z}_8/\langle 2\rangle$

- List the elements.
  $\{c_0, c_1\}$ where
  $c_0 = 0 + \langle 2\rangle = \{0, 2, 4, 6\}$
  $c_1 = 1 + \langle 2\rangle = \{1, 3, 5, 7\}$
- Construct the operation tables for addition and multiplication

$+$	c_0	c_1	$\cdot$	c_0	c_1
c_0	c_0	c_1	c_0	c_0	c_0
c_1	c_1	c_0	c_1	c_0	c_1

- Verify that it is a ring.
  Obvious from the tables.

(c) $\mathbb{Z}_8/\langle 4\rangle$

- List the elements.
  $\{c_0, c_1, c_2, c_3\}$ where
  $c_0 = 0 + \langle 4\rangle = \{0, 4\}$
  $c_1 = 1 + \langle 4\rangle = \{1, 5\}$
  $c_2 = 2 + \langle 4\rangle = \{2, 6\}$
  $c_3 = 3 + \langle 4\rangle = \{3, 7\}$
- Construct the operation tables for addition and multiplication

$+$	c_0	c_1	c_2	c_3	$\cdot$	c_0	c_1	c_2	c_3
c_0	c_0	c_1	c_2	c_3	c_0	c_0	c_0	c_0	c_0
c_1	c_1	c_2	c_3	c_0	c_1	c_0	c_1	c_2	c_3
c_2	c_2	c_3	c_0	c_1	c_2	c_0	c_2	c_0	c_2
c_3	c_3	c_0	c_1	c_2	c_3	c_0	c_3	c_2	c_1

- Verify that it is a ring.
  Obvious from the tables.

(d) $\mathbb{Z}_2[x] / \langle x \rangle$

- List the elements.
  $\{c_0, c_1\}$ where
  $c_0 = 0 + \langle x \rangle = \{0, x, \quad x^2, x^2 + x^1, \quad x^3, x^3 + x^1, x^3 + x^2, x^3 + x^2 + x^1, \ \ldots\}$
  $c_1 = 1 + \langle x \rangle = \{1, x+1, \quad x^2+1, x^2 + x^1 + 1, \quad x^3+1, x^3 + x^1 + 1, x^3 + x^2 + 1, x^3 + x^2 + x^1 + 1, \ \ldots\}$
- Construct the operation tables for addition and multiplication

$+$	c_0	c_1	$\cdot$	c_0	c_1
c_0	c_0	c_1	c_0	c_0	c_0
c_1	c_1	c_2	c_1	c_0	c_1

- Verify that it is a ring.
  Obvious from the tables.

(e) $\mathbb{Z}_2[x] / \langle x^2 \rangle$

- List the elements.
  $\{c_0, c_1, c_x, c_{x+1}\}$ where
  $c_0 = 0 + \langle x^2 \rangle = \{0, x^2, \quad x^3, x^3 + x^2, \ x^4 + x^2, x^4 + x^3, x^4 + x^3 + x^2, \ldots\}$
  $c_1 = 1 + \langle x^2 \rangle = \{1, x^2 + 1, \quad x^3 + 1, x^3 + x^2 + 1, \quad x^4 + 1, x^4 + x^2 + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + 1, \ldots\}$
  $c_x = x + \langle x^2 \rangle = \{x, x^2 + x, \quad x^3 + x, x^3 + x^2 + x, \quad x^4 + x, x^4 + x^2 + x, x^4 + x^3 + x, x^4 + x^3 + x^2 + x, \ldots\}$
  $c_{x+1} = x + 1 + \langle x^2 \rangle = \{x + 1, x^2 + x + 1, \quad x^3 + x + 1, x^3 + x^2 + x + 1, \quad x^4 + x + 1, x^4 + x^2 + x + 1, x^4 + x^3 +$
- Construct the operation tables for addition and multiplication

$+$	c_0	c_1	c_x	c_{x+1}	$\cdot$	c_0	c_1	c_x	c_{x+1}
c_0	c_0	c_1	c_x	c_{x+1}	c_0	c_0	c_0	c_0	c_0
c_1	c_1	c_0	c_{x+1}	c_x	c_1	c_0	c_1	c_x	c_{x+1}
c_x	c_x	c_{x+1}	c_0	c_1	c_x	c_0	c_x	c_0	c_x
c_{x+1}	c_{x+1}	c_x	c_1	c_0	c_{x+1}	c_0	c_{x+1}	c_x	c_1

- Verify that it is a ring.
  Obvious from the tables.

5. Prove: Let R be a CRU and let $a_1, \ldots, a_n \in R$. Then $\langle a_1, \ldots, a_n \rangle \lhd R$.

6. Prove: Let R be a ring and let $I \lhd R$. Then the addition operation on R/I is well defined.

7. Prove: Let R be a ring and let $I \lhd R$. Then the multiplication operation on R/I is well defined.

8. Prove: Let R be a ring and let $I \lhd R$. Then R/I is a ring.

2.6 Homomorphism, Isomorphism, Image and Kernel

1. State the definition of the following notions

   (a) Homomorphism
   Let $(R, +, \cdot)$ and $(R', +', \cdot')$ be rings. Let $\phi : R \longrightarrow R'$. We say that ϕ is a homomorphism iff $\forall a, b \in R\ \phi(a+b) = \phi(a) +' \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot' \phi(b)$.

   (b) Isomorphism
   ϕ is called an isomorphism iff it is homomorphism, one-to-one and onto.

   (c) Isomorphic ($\cong$)
   $R \cong R'$ iff there is an isomorphism $\phi : R \longrightarrow R'$.

   (d) Kernel
   Let $(R, +, \cdot)$ and $(R', +', \cdot')$ be rings. Let $\phi : R \longrightarrow R'$. Then $\ker \phi = \{a \in R : \phi(a) = 0'\}$.

   (e) Image
   Let $(R, +, \cdot)$ and $(R', +', \cdot')$ be rings. Let $\phi : R \longrightarrow R'$. Then $\operatorname{im} \phi = \{\phi(a) : a \in R\}$.

2. For each of the following maps $\phi : (R, +, \cdot) \longrightarrow (R', +', \cdot')$ do

   (a) $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_5$, given by $x \longmapsto x \bmod 5$

   - Draw the map diagram for ϕ.

     $\vdots$
     $-5 \longrightarrow 0$
     $-4 \longrightarrow 1$
     $-3 \longrightarrow 2$
     $-2 \longrightarrow 3$
     $-1 \longrightarrow 4$
     $+0 \longrightarrow 0$
     $+1 \longrightarrow 1$
     $+2 \longrightarrow 2$
     $+3 \longrightarrow 3$
     $+4 \longrightarrow 4$
     $+5 \longrightarrow 0$
     $\vdots$

   - Construct the operation tables for $\operatorname{im} \phi$.

+	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

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

   - Construct the operation tables for $\ker \phi$.

+	$\cdots$	-5	0	5	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
-5	$\cdots$	-10	-5	0	$\cdots$
0		-5	0	5	
5	$\cdots$	0	5	10	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	

$\cdot$	$\cdots$	-5	0	5	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
-5	$\cdots$	25	0	-25	$\cdots$
0		0	0	0	
5	$\cdots$	-25	0	25	$\cdots$
$\vdots$		$\vdots$		$\vdots$	

- Construct the operation tables of $R/\ker\phi$.
  Let $c_i = i + 5\mathbb{Z}$.

$+$	c_0	c_1	c_2	c_3	c_4
c_0	c_0	c_1	c_2	c_3	c_4
c_1	c_1	c_2	c_3	c_4	c_0
c_2	c_2	c_3	c_4	c_0	c_1
c_3	c_3	c_4	c_0	c_1	c_2
c_4	c_4	c_0	c_1	c_2	c_3

$\cdot$	c_0	c_1	c_2	c_3	c_4
c_0	c_0	c_0	c_0	c_0	c_0
c_1	c_0	c_1	c_2	c_3	c_4
c_2	c_0	c_2	c_4	c_1	c_3
c_3	c_0	c_3	c_1	c_4	c_2
c_4	c_0	c_4	c_3	c_2	c_1

- Draw the map diagram for the "natural" isomorphism that shows $R/\ker\phi \cong \operatorname{im}\phi$
  $c_0 \longrightarrow 0$
  $c_1 \longrightarrow 1$
  $c_2 \longrightarrow 2$
  $c_3 \longrightarrow 3$
  $c_4 \longrightarrow 4.$

(b) $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_{10}$, given by $x \longmapsto (5x) \bmod 10$

- Draw the map diagram for ϕ.
  $0 \longrightarrow 0$
  $1 \longrightarrow 5$
  $2 \longrightarrow 0$
  $3 \longrightarrow 5$
- Construct the operation tables for $\operatorname{im}\phi$.

$+$	0	5
0	0	5
5	5	0

$\cdot$	0	5
0	0	0
5	0	5

- Construct the operation tables for $\ker\phi$.

$+$	0	2
0	0	2
2	2	0

$\cdot$	0	2
0	0	0
2	0	0

- Construct the operation tables of $R/\ker\phi$.
  Let $c_0 = \{0, 2\}$ and $c_1 = \{1, 3\}$.

$+$	c_0	c_1
c_0	c_0	c_1
c_1	c_1	c_0

$\cdot$	c_0	c_1
c_0	c_0	c_0
c_1	c_0	c_1

- Draw the map diagram for the "natural" isomorphism that shows $R/\ker\phi \cong \operatorname{im}\phi$
  $c_0 \longrightarrow 0$
  $c_1 \longrightarrow 5$

(c) $\phi : \mathbb{Z}_5 \longrightarrow \mathbb{Z}_{10}$, given by $x \longmapsto (6x) \bmod 10$

- Draw the map diagram for ϕ.
  $0 \longrightarrow 0$
  $1 \longrightarrow 6$
  $2 \longrightarrow 2$
  $3 \longrightarrow 8$
  $4 \longrightarrow 4$
- Construct the operation tables for $\operatorname{im}\phi$.

$+$	0	6	2	8	4
0	0	6	2	8	4
6	6	2	8	4	0
2	2	8	4	0	6
8	8	4	0	6	2
4	4	0	6	2	8

$\cdot$	0	6	2	8	4
0	0	0	0	0	0
6	0	6	2	8	4
2	0	2	4	6	8
8	0	8	6	4	2
4	0	4	8	2	6

- Construct the operation tables for $\ker\phi$.

$+$	0
0	0

$\cdot$	0
0	0

- Construct the operation tables of $R/\ker\phi$.

Let $c_i = i + \{0\} = \{i\}$.

$+$	c_0	c_1	c_2	c_3	c_4
c_0	c_0	c_1	c_2	c_3	c_4
c_1	c_1	c_2	c_3	c_4	c_0
c_2	c_2	c_3	c_4	c_0	c_1
c_3	c_3	c_4	c_0	c_1	c_2
c_4	c_4	c_0	c_1	c_2	c_3

$\cdot$	c_0	c_1	c_2	c_3	c_4
c_0	c_0	c_0	c_0	c_0	c_0
c_1	c_0	c_1	c_2	c_3	c_4
c_2	c_0	c_2	c_4	c_1	c_3
c_3	c_0	c_3	c_1	c_4	c_2
c_4	c_0	c_4	c_3	c_2	c_1

- Draw the map diagram for the "natural" isomorphism that shows $R/\ker\phi \cong \operatorname{im}\phi$

$c_0 \longrightarrow 0$
$c_1 \longrightarrow 6$
$c_2 \longrightarrow 2$
$c_3 \longrightarrow 8$
$c_4 \longrightarrow 4$

3. Prove: Let $(R,+,\cdot)$ and $(R',+',\cdot')$ be rings. Let $\phi : R \longrightarrow R'$ be a homomorphism. Then $\phi(0) = 0'$.

4. Prove: Let $(R,+,\cdot)$ and $(R',+',\cdot')$ be rings. Let $\phi : R \longrightarrow R'$ be a homomorphism. Then $\phi(-a) = -'\phi(a)$.

5. Prove: Let $(R,+,\cdot)$ and $(R',+',\cdot')$ be rings. Let $\phi : R \longrightarrow R'$ be a homomorphism. Then $\operatorname{im}\phi \le R'$.

6. Prove: Let $(R,+,\cdot)$ and $(R',+',\cdot')$ be rings. Let $\phi : R \longrightarrow R'$ be a homomorphism. Then $\ker\phi \le R$.

7. Prove: Let $(R,+,\cdot)$ and $(R',+',\cdot')$ be rings. Let $\phi : R \longrightarrow R'$ be a homomorphism. Then $\ker\phi \lhd R$.

8. Prove: Let $(R,+,\cdot)$ and $(R',+',\cdot')$ be rings. Let $\phi : R \longrightarrow R'$ be a homomorphism. Then $R/\ker\phi \cong \operatorname{im}\phi$.