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

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

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

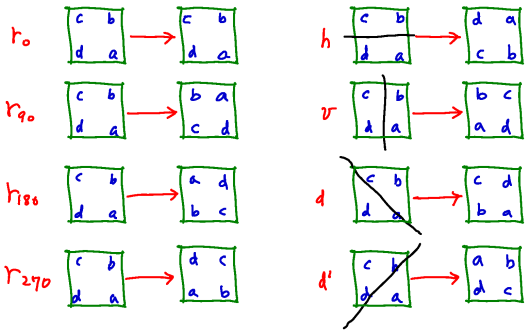
   (c) $(S_3, \ \circ)$

$a\backslash b$	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 $p_0 = \begin{bmatrix} 123 \\ 123 \end{bmatrix}$ $p_1 = \begin{bmatrix} 123 \\ 231 \end{bmatrix}$ $p_2 = \begin{bmatrix} 123 \\ 312 \end{bmatrix}$
$p_3 = \begin{bmatrix} 123 \\ 132 \end{bmatrix}$ $p_4 = \begin{bmatrix} 123 \\ 321 \end{bmatrix}$ $p_5 = \begin{bmatrix} 123 \\ 213 \end{bmatrix}$

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

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

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

   - 1
a	1	3	5	7
a^{-1}	1	3	5	7

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

   - p_0
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

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

   - r_0
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'

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.

  $S = \{r_0\}$

  $r_0S = \{r_0\} = Sr_0$

  $r_{90}S = \{r_{90}\} = Sr_{90}$

  $r_{180}S = \{r_{180}\} = Sr_{180}$

  $r_{270}S = \{r_{270}\} = Sr_{270}$

  $hS = \{h\} = Sh$

  $vS = \{v\} = Sv$

  $dS = \{d\} = Sd$

  $d'S = \{d'\} = Sd'$

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

  $r_0S = r_{180}S = \{r_0, r_{180}\} = Sr_0 = Sr_{180}$

  $r_{90}S = r_{270}S = \{r_{90}, r_{270}\} = Sr_{90} = Sr_{270}$

  $hS = vS = \{h, v\} = Sh = Sv$

  $dS = d'S = \{d, d'\} = Sd = Sd'$

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

  $r_0S = r_{90}S = r_{180}S = r_{270}S = \{r_0, r_{90}, r_{180}, r_{270}\} = Sr_0 = Sr_{90} = Sr_{180} = Sr_{270}$

  $hS = dS = vS = d'S = \{h, d, v, d'\} = Sh = Sv = Sd = Sd'$

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

  $r_0S = r_{180}S = hS = vS = \{r_0, r_{180}, h, v\} = Sr_0 = Sr_{180} = Sh = Sv$

  $r_{90}S = r_{270}S = d'S = dS = \{r_{90}, r_{270}, d', d\} = Sr_{90} = Sr_{270} = Sd = Sd'$

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

  $r_0S = r_{180}S = dS = d'S = \{r_0, r_{180}, d, d'\} = Sr_0 = Sr_{180} = Sd = Sd'$

  $r_{90}S = r_{270}S = hS = vS = \{r_{90}, r_{270}, h, v\} = Sr_{90} = Sr_{270} = Sh = Sv$

  $S = D_4$

  $r_0S = r_{90}S = r_{180}S = r_{270}S = hS = vS = dS = d'S = D_4 =$
  $Sr_0 = Sr_{90} = Sr_{180} = Sr_{270} = Sh = Sv = Sd = Sd'$

- 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 $\forall a, b \in G \quad \phi(a \circ b) = \phi(a) \circ' \phi(b)$.

   (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.

     $0 \mapsto 0$
     $1 \mapsto 3$
     $2 \mapsto 6$
     $3 \mapsto 0$
     $4 \mapsto 3$
     $5 \mapsto 6$
     $6 \mapsto 0$
     $7 \mapsto 3$
     $8 \mapsto 6$

   - 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 $G/\ker\phi \cong \operatorname{im}\phi$.
  $\{0,3,6\} \mapsto 0$
  $\{1,4,7\} \mapsto 3$
  $\{2,5,8\} \mapsto 6$

(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.
  $1 \mapsto 1$
  $3 \mapsto 1$
  $5 \mapsto 5$
  $7 \mapsto 5$
- Verify that ϕ is a homomorphism.
  Obvious from the diagram.
- Construct the operation table for $\operatorname{im}\phi$, and verify that $\operatorname{im}\phi \leq G'$.

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

  Obvious from the table that $\operatorname{im}\phi \leq U_8$.
- 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 $G/\ker\phi \cong \operatorname{im}\phi$.
  $\{1,3\} \mapsto 1$
  $\{5,7\} \mapsto 5$

(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.
  $p_0 \mapsto 1$
  $p_1 \mapsto 1$
  $p_2 \mapsto 1$
  $p_3 \mapsto 3$
  $p_4 \mapsto 3$
  $p_5 \mapsto 3$
- Verify that ϕ is a homomorphism.
  Obvious from the diagram.
- Construct the operation table for $\operatorname{im}\phi$, and verify that $\operatorname{im}\phi \leq G'$.

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

  Obvious from the table that $\operatorname{im}\phi \leq U_8$.
- 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 $G/\ker\phi \cong \operatorname{im}\phi$.

$\{p_0,p_1,p_2\} \mapsto 1$
$\{p_3,p_4,p_5\} \mapsto 3$

(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.

$r_0 \mapsto 0$
$r_{90} \mapsto 0$
$r_{180} \mapsto 0$
$r_{270} \mapsto 0$
$h \mapsto 2$
$v \mapsto 2$
$d \mapsto 2$
$d' \mapsto 2$

- 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 $G/\ker\phi \cong \operatorname{im}\phi$.

$\{r_0,r_{90},r_{180},r_{270}\} \mapsto 0$
$\{h,v,d,d'\} \mapsto 2$

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

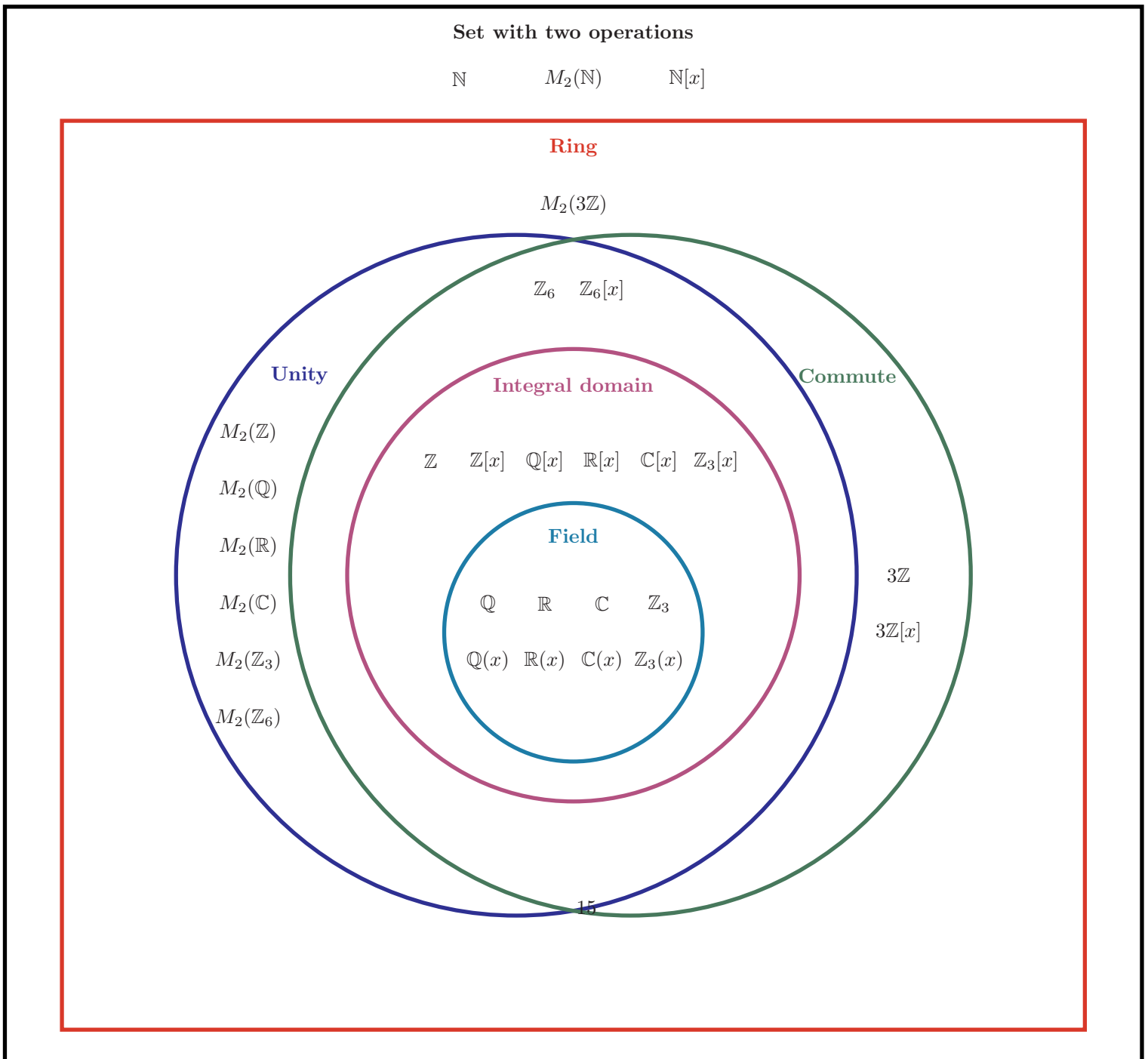
   (b) $M_n(S)$ = the set of all n by n matrices with the entries from the set S.

   (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 $\mathbb{Z}_2[x]$
$\left\{0, x, \quad x^2, x^2 + x^1, \quad x^3, x^3 + x^1, x^3 + x^2, x^3 + x^2 + x^1, \ \ldots\right\}$

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

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
  $c_0 = 0 + \langle x\rangle = \{0, x,\ \ x^2, x^2+x^1,\ \ x^3, x^3+x^1, x^3+x^2, x^3+x^2+x^1,\ \ldots\}$
  $c_1 = 1 + \langle x\rangle = \{1, x+1,\ \ x^2+1, x^2+x^1+1,\ \ x^3+1, x^3+x^1+1, x^3+x^2+1, x^3+x^2+x^1+1,\ \ldots\}$
- 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_0	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
  $c_0 = 0 + \langle x^2\rangle = \{0, x^2,\ \ x^3, x^3+x^2,\ x^4+x^2, x^4+x^3, x^4+x^3+x^2, \ldots\}$
  $c_1 = 1 + \langle x^2\rangle = \{1, x^2+1,\ \ x^3+1, x^3+x^2+1,\ \ x^4+1, x^4+x^2+1, x^4+x^3+1, x^4+x^3+x^2+1, \ldots\}$
  $c_x = x + \langle x^2\rangle = \{x, x^2+x,\ \ x^3+x, x^3+x^2+x,\ \ x^4+x, x^4+x^2+x, x^4+x^3+x, x^4+x^3+x^2+x, \ldots\}$
  $c_{x+1} = x+1 + \langle x^2\rangle = \{x+1, x^2+x+1,\ \ x^3+x+1, x^3+x^2+x+1,\ \ x^4+x+1, x^4+x^2+x+1, x^4+x^3+$
- 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	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	

$+$	$\cdots$	-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 $\operatorname{im} \phi \leq R'$.

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

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 $R/\ker \phi \cong \operatorname{im} \phi$.

3 Applications and Related advanced topics

3.1 Cryptography (ElGamal)

1. Describe the ElGamal Scheme.

   1985 IEEE Transaction on information theory, Cited: 1800 PhD Stanford 1984

   Alice wants to send a message to Bob, securely and efficiently.

   Bob does the following once.

   (a) Chooses a group G
   (b) Choose $g \in G$
   (c) Choose a natural number k
   (d) Compute $h = g^k$
   (e) Tell the whole world: G, g, h.

   Alice does the following whenever she wants to send a message to Bob.

   (a) Encode the message as $m \in G$ using an international standard.
   (b) Choose a natural number s.
   (c) Encrypt m into $c_1 = g^s$ and $c_2 = h^s m$.
   (d) Sends to Bob (using insecure channel): c_1, c_2.

   Bob does the following upon receiving series of c_1, c_2 from Alice.

   (a) Decrypt c_1 and c_2 into $m' = c_1^{-k} c_2$.
   (b) Decode m' using the international standard.

2. Suppose that $G = U_7$, $g = 2$, $k = 5$, $m = 3$, $s = 4$. Determine the values of h, c_1, c_2 and m'.

   - $h = g^k = 2^5 = 4$
   - $c_1 = g^s = 2^4 = 2$
   - $c_2 = h^s m = 4^4 \cdot 3 = 5$
   - $m' = c_1^{-k} c_2 = 2^{-5} \cdot 5 = 4^5 \cdot 5 = 3$

3. Suppose that $G = U_{13}$, $g = 4$, $k = 5$, $m = 6$, $s = 2$. Determine the values of h, c_1, c_2 and m'.

   - $h = g^k = 4^5 = \text{rem}\left(4^5, 13\right) = 10$
   - $c_1 = g^s = 4^2 = \text{rem}\left(4^2, 13\right) = 3$
   - $c_2 = h^s m = 10^2 \cdot 6 = \text{rem}\left(10^2 \cdot 6, 13\right) = 2$
   - $m' = c_1^{-k} c_2 = 3^{-5} \cdot 2 = 9^5 \cdot 2 = \text{rem}\left(9^5 \cdot 2, 13\right) = 6$

4. Prove: The ElGamal scheme is correct, that is, $m' = m$.

3.2 Elliptic curve group

1. Let F be a field and let $a, b \in F$. State the definition of Elliptic curve E.

$$E = \left\{(x, y) \in F^2 : y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

2. State the formal definition of the operation on E.

   Let $p,\ q \in E$. Then $s = p + q$ is defined by

If	$p = \infty$	:	$s = q$
Else if	$q = \infty$	:	$s = p$
Else if	$x_p = x_q$ and $y_p = -y_q$	:	$s = \infty$
Else if	$x_p = x_q$ and $y_p = y_q$	:	$m = \frac{3x_p^2 + a}{2y_p}$ $x_s = m^2 - x_p - x_q$ $y_s = -y_p - m(x_s - x_p)$
Else	(generic case)	:	$m = \frac{y_q - y_p}{x_q - x_p}$ $x_s = m^2 - x_p - x_q$ $y_s = -y_p - m(x_s - x_p)$

3. Let $F = (\mathbb{Z}_3, +_3, \times_3)$ and $a = 1$ and $b = 1$.

   (a) Find all the elements of the elliptic curve E.

$$\begin{aligned} E &= \left\{(x, y) \in \mathbb{Z}_3^2 : y^2 = x^3 + x + 1\right\} \cup \{\infty\} \\ &= \{(0,1), (0,2), (1,0), \infty\} \end{aligned}$$

   (b) Construct the operation table.

$$\begin{bmatrix} op & (0,1) & (0,2) & (1,0) & \infty \\ (0,1) & (1,0) & \infty & (0,2) & (0,1) \\ (0,2) & \infty & (1,0) & (0,1) & (0,2) \\ (1,0) & (0,2) & (0,1) & \infty & (1,0) \\ \infty & (0,1) & (0,2) & (1,0) & \infty \end{bmatrix}$$

4. Let $F = (\mathbb{Z}_5, +_5, \times_5)$ and $a = 0$ and $b = 1$.

   (a) Find all the elements of the elliptic curve E.
   Note

$$\begin{aligned} E &= \left\{(x, y) \in \mathbb{Z}_5^2 : y^2 = x^3 + 0x + 1\right\} \cup \{\infty\} \\ &= \{(0,1), (0,4), (2,2), (2,3), (4,0), \infty\} \end{aligned}$$

   (b) Construct the operation table.

$$\begin{bmatrix} op & (0,1) & (0,4) & (2,2) & (2,3) & (4,0) & \infty \\ (0,1) & (0,4) & \infty & (2,3) & (4,0) & (2,2) & (0,1) \\ (0,4) & \infty & (0,1) & (4,0) & (2,2) & (2,3) & (0,4) \\ (2,2) & (2,3) & (4,0) & (0,4) & \infty & (0,1) & (2,2) \\ (2,3) & (4,0) & (2,2) & \infty & (0,1) & (0,4) & (2,3) \\ (4,0) & (2,2) & (2,3) & (0,1) & (0,4) & \infty & (4,0) \\ \infty & (0,1) & (0,4) & (2,2) & (2,3) & (4,0) & \infty \end{bmatrix}$$

5. Derive the formulas for $m, x_s$and y_s for the generic case from the "geometric/informal" definition.

6. Derive the formula for the slope m when $x_p = x_q$ and $y_p = y_q$ from the "geometric/informal" definition.

7. Prove: $(E, +)$ is a commutative group.

3.3 Multiplicative inverse in $\mathbb{Z}_p$

1. State an algorithm for multiplicative inverse in $\mathbb{Z}_p$.

   In: $a \in \mathbb{Z}_p \setminus \{0\}$

   Out: a^{-1}

   (a) $r_0 = p,\ t_0 = 0$
   $r_1 = a,\ t_1 = 1$

   (b) For $i = 2, \ldots$ do

   i. $q_i = \text{quo}\,(r_{i-2}, r_{i-1})$
   ii. $r_i = \text{rem}\,(r_{i-2}, r_{i-1})$
   iii. $t_i = t_{i-2} - q_i t_{i-1} \bmod p$
   iv. if $r_i = 0$ then exit from the loop.

   (c) Return t_{i-1}.

2. Find 4^{-1} in $\mathbb{Z}_7$ using the algorithm.

   See the trace of the algorithm:

i	q_i	r_i	t_i
0		7	0
1		4	1
2	1	3	6
3	1	1	2
4	3	0	0

   Note that $r_4 = 0$. Thus $4^{-1} = t_3 = 2$.

3. Find 7^{-1} in $\mathbb{Z}_{11}$ using the algorithm.

   See the trace of the algorithm:

i	q_i	r_i	t_i
0		11	0
1		7	1
2	1	4	10
3	1	3	2
4	1	1	8
5	3	0	0

   Note that $r_5 = 0$. Thus $7^{-1} = t_4 = 8$.

4. Prove: The algorithm is correct.

   The proof can be divided into proving the following claims:

   (a) Prove: $\forall i \geq 0 \quad at_i = r_i \bmod p$.

   (b) Prove: $\forall i \geq 1 \quad \gcd\,(r_{i-1}, r_i) = 1$.

   (c) Prove: If $r_i = 0$ then $r_{i-1} = 1$.

   (d) Prove: If $r_i = 0$ then $at_{i-1} = 1 \bmod p$, hence $t_{i-1} = a^{-1}$.

   (e) Prove: $\exists i \geq 1\ r_i = 0$.

3.4 Multiplicative inverse in $GF(p^n)$

1. State an algorithm for multiplicative inverse in $GF(p^n)$.

   In: $a \in GF(p^n) \setminus \{0\}$, $h \in \mathbb{Z}_p[v]$ irreducible

   Out: a^{-1}

   (a) $r_0 = h$, $t_0 = 0$
   $r_1 = a$, $t_1 = 1$

   (b) For $i = 2, \ldots$ do

   i. $q_i, r_i = \text{quo-rem}(r_{i-2}, r_{i-1})$
   ii. $t_i = t_{i-2} - q_i t_{i-1} \bmod h$
   iii. If $r_i = 0$ then return t_{i-1}/r_{i-1}.

2. Find $(v+1)^{-1}$ in $GF(2^2)$ where $h = v^2 + v + 1$ using the algorithm.

   See the trace of the algorithm:

i	q_i	r_i	t_i
0		v^2+v+1	0
1		$v+1$	1
2	v	1	v
3	$v+1$	0	0

   Note that $r_3 = 0$. Thus $(v+1)^{-1} = t_2/r_2 = v/1 = v$

3. Find $(v^2+2)^{-1}$ in $GF(3^4)$ where $h = v^4 + 2v^3 + 2$ using the algorithm.

   See the trace of the algorithm:

i	q_i	r_i	t_i
0		v^4+2v^3+2	0
1		v^2+2	1
2	v^2+2v+1	$2v$	$2v^2+v+2$
3	$2v$	2	$2v^3+v^2+2v+1$
4	v	0	0

   Note that $r_4 = 0$. Thus $(v^2+2)^{-1} = t_3/r_3 = v^3 + 2v^2 + v + 2$.

4. Prove: The algorithm is correct.

   The proof can be divided into proving the following claims:

   (a) Prove: $\forall i \geq 0 \quad t_i a =_h r_i$.
   (b) Prove: $\forall i \geq 1 \quad \deg \gcd(r_{i-1}, r_i) = 0$.
   (c) Prove: If $r_i = 0$ then $\deg r_{i-1} = 0$.
   (d) Prove: If $r_i = 0$ then $\deg(t_{i-1}a) = 0$, hence $a^{-1} = t_{i-1}/r_{i-1}$.
   (e) Prove: $\exists i \geq 1 \; r_i = 0$.

3.5 Maximal ideal, Quotient ring, Field

1. Define: maximal ideal.

   Let R be a ring. Let $I \lhd R$. We say that I is maximal iff

   (a) $I \neq R$

   (b) $\nexists J \lhd R \;\; I \subsetneq J \subsetneq R$ (equivalently $\forall J \lhd R$ if $I \subsetneq J$ then $J = R$).

2. Prove: Let R be a CRU with $0 \neq 1$ and $I \lhd R$. Then R/I is a field if and only if I is a maximal ideal of R.

3. Prove: Let F be a field. Let $h \in F[v]$ be irreducible. Then $\langle h \rangle$ is a maxmal ideal of $F[v]$.

4. Prove: Let F be a field. Let $h \in F[v]$ be irreducible. Then $F[v] / \langle h \rangle$ is a field.

5. Prove: Let $h \in \mathbb{Z}_p[v]$ be irreducible. Let $\phi : \mathbb{Z}_p[v] \longrightarrow \mathbb{Z}_p[v]$ such that $f \longmapsto \text{rem}(f, h)$. Then

   (a) ϕ is a homomorphism.

   (b) im $\phi = GF(p^n)$, that is $F_{p,n}$

   (c) ker $\phi = \langle h \rangle$

6. Prove: $F_{p,n}$ is a field.

3.6 Radical formula for roots of polynomials

1. Write down the radical formulas in the coefficients for the roots of

$$f = x^d + a_{d-1}x^{d-1} + \cdots + a_0 x^0 = 0$$

for $d = 2, 3, 4$.

- $d = 2$: Sridhard around 800 AD
  $x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}$
  can be rewritten as
  $\begin{cases} t_1^2 &= a_1^2 - 4a_0 \\ x &= \left(-a_1 + t_1\right)/2 \end{cases}$
- $d = 3$: Tartaglia-Ferro around 1500 AD
  $\begin{cases} t_1^2 &= \left(9a_1a_2 - 27a_0 - 2a_2^3\right)^2 - 4\left(a_2^2 - 3a_1\right) \\ t_2^3 &= \left(9a_1a_2 - 27a_0 - 2a_2^3 + t_1\right)/2 \\ x &= \left(a_2^2 - 3a_1 - a_2t_2 + t_2^2\right)/3t_2 \end{cases}$
- $d = 4$: Ferrari around1500 AD
  $\begin{cases} t_1^2 &= 108\,a_1^2a_2^3 + 729\,a_0^2a_3^4 + 3456\,a_0^2a_2^2 - 432\,a_0a_2^4 + 108\,a_1^3a_3^3 + 729\,a_1^4 \\ & \quad -6912\,a_0^3 - 486\,a_0a_3^3a_2a_1 + 2160\,a_0a_2^2a_1a_3 + 162\,a_1^2a_0a_3^2 - 3888\,a_1^2a_0a_2 \\ & \quad -486\,a_1^3a_2a_3 - 3888\,a_0^2a_3^2a_2 + 108\,a_0a_3^2a_2^3 - 27\,a_2^2a_1^2a_3^2 + 5184\,a_1a_3a_0^2 \\ t_2^3 &= 32\left(-72a_0a_2 - 9a_1a_2a_3 + 27a_1^2 + 2a_2^3 + 27a_0a_3^2 + t_1\right) \\ t_3^2 &= \left(16\left(12a_0 - 3a_1a_3 + a_2^2\right) + \left(3a_3^2 - 8a_2\right)t_2 + t_2^2\right)/\left(3t_2\right) \\ t_4^2 &= \left(\left(24a_2a_3 - 48a_1 - 6a_3^3\right)t_2 + \left(48a_1a_3 - 192a_0 - 16a_2^2\right)t_3 + \left(6a_3^2 - 16a_2\right)t_2t_3 - t_2^2t_3\right)/\left(12t_2t_3\right) \\ x &= \left(a_3 + t_3 + 2t_4\right)/4 \end{cases}$

2. Rewrite the formulas in terms of roots of f.

- $d = 2$:
  $\begin{cases} t_1 &= r_1 - r_2 \\ x &= r_1 \end{cases}, \begin{cases} t_1 &= r_2 - r_1 \\ x &= r_2 \end{cases}$
- $d = 3$:
  $\begin{cases} t_1 &= \sqrt{27}\omega_2\left(r_1 - r_2\right)\left(r_1 - r_3\right)\left(r_2 - r_3\right) \\ t_2 &= \left(r_1 + \omega_3 r_2 + \omega_3^2 r_3\right) \\ x &= r_1 \end{cases}, \ldots$
  where $\omega_k = e^{2\pi i/k}$
- $d = 4$:
  $\begin{cases} t_1 &= \sqrt{27}\omega_2\left(r_1 - r_2\right)\left(r_1 - r_3\right)\left(r_1 - r_4\right)\left(r_2 - r_3\right)\left(r_2 - r_4\right)\left(r_3 - r_4\right) \\ t_2 &= \left(r_1 + r_2 - r_3 - r_4\right)^2 + \omega_3\left(r_1 + r_3 - r_2 - r_4\right)^2 + \omega_3^2\left(r_1 + r_4 - r_2 - r_3\right) \\ t_3 &= r_1 + r_2 - r_3 - r_4 \\ t_4 &= r_1 - r_2 \\ x &= r_1 \end{cases}$

3. Find the groups of symmetries, that is,

$$G_0 = S_d$$
$$G_k = \{\pi \in G_{k-1} : \pi\left(t_k\right) = t_k\}$$

where

$$\pi\left(t_k\left(r_1, \ldots, r_d\right)\right) = t_k\left(r_{\pi_1}, \ldots, r_{\pi_d}\right).$$

- $d = 2$:
  $G_0 = S_2$
  $G_1 = \{e\}$
- $d = 3$:
  $G_0 = S_3$
  $G_1 = A_3$
  $G_2 = \{e\}$
- $d = 4$:
  $G_0 = S_4$
  $G_1 = A_4$
  $G_2 = \left\{ \begin{bmatrix} 1234 \\ 1234 \end{bmatrix}, \begin{bmatrix} 1234 \\ 2143 \end{bmatrix}, \begin{bmatrix} 1234 \\ 3412 \end{bmatrix}, \begin{bmatrix} 1234 \\ 4321 \end{bmatrix} \right\}$
  $G_3 = \left\{ \begin{bmatrix} 1234 \\ 1234 \end{bmatrix}, \begin{bmatrix} 1234 \\ 2143 \end{bmatrix} \right\}$
  $G_4 = \{e\}$

4. Find the relationship among the groups.

   - $d = 2$:
     (a) $|G_0| / |G_1| = 2$
     (b) $G_0 \rhd G_1$
   - $d = 3$:
     (a) $G_0 \rhd G_1 \rhd G_2$
     (b) $|G_0| / |G_1| = 2$
     $|G_1| / |G_2| = 3$
   - $d = 4$:
     (a) $G_0 \rhd G_1 \rhd G_2 \rhd G_3 \rhd G_4$
     (b) $|G_0| / |G_1| = 2$
     $|G_1| / |G_2| = 3$
     $|G_2| / |G_3| = 2$
     $|G_3| / |G_4| = 2$

5. Abstract the findings to arbitrary degree d.

   Theorem: If there is a radical formula for the solution of $f = x^d + a_{d-1}x^{d-1} + \cdots + a_0x^0 = 0$ then there exists subsets of $G_1, \ldots, G_{\ell-1}$ of S_d such that

   (a) $S_d = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_\ell = \{e\}$
   (b) $|G_{k-1}| / |G_k|$ is prime for every $k \geq 1$.

6. Apply the theorem to $d = 5$.

   (a) Find the normal subgroups of S_5.
   $G_0 = S_5$
   $G_1 = A_5$
   $G_2 = \{e\}$
   (b) Study the relationship among the groups.
   i. $G_0 \rhd G_1 \rhd G_2$
   ii. $\frac{|G_0|}{|G_1|} = \frac{120}{60} = 2$
   $\frac{|G_1|}{|G_2|} = \frac{60}{1} = 60$

(c) Say about the existence of radical formula.
Note that 60 is *not* a prime.
Thus we conclude that there is no radical formula for $d = 5$.