

# Homework 1.

Exercise 1.1. Prove that  $(a * b) * c = c * (a * b)$  for any  $a, b, c \in X$  if  $*$  is an associative commutative operation on  $X$ .

$$\begin{aligned} \text{Pf: } (a * b) * c &= c * (a * b) && \text{by commutative. of } * \\ &= c * (b * a) && \text{by commutative again.} \end{aligned}$$

thus RHS = LHS

Exercise 1.2. Let  $X = \mathbb{R}$  and  $a * b = a + b + ab$ .

- i) Is the operation  $*$  associative?
- ii) Does the operation  $*$  possess an identity element?
- iii) Find all  $x \in X$  which are not invertible.

Pf: (i). Yes.  $\forall a, b, c \in \mathbb{R}$ .

$$(a * b) * c = (a + b + ab) * c = a + b + c + ab + (a + b + ab)c = a + b + c + ab + ac + bc + abc$$

$$a * (b * c) = a * (b + c + bc) = a + b + c + bc + a(b + c + bc) = a + b + c + bc + ab + ac + abc$$

by the commutative of "+",  $(a * b) * c = a * (b * c)$

(ii). Yes. we claim that identity element is  $0 \in \mathbb{R}$ .

$$a * 0 = a + 0 + 0 = a \quad 0 * a = 0 + a + 0 = a.$$

i.e.  $a * 0 = 0 * a = a$ .

(iii).  $\forall a \in X$  assume  $b$  is its inverse

$$\text{i.e. } a + b + ab = 0 \text{ and } b + a + ba = 0 \Rightarrow b = \frac{-a}{1+a}$$

this number not exist in  $\mathbb{R}$ . iff  $1+a=0$  i.e.  $a=-1$ .

the not invertible set is  $\{-1\}$ .

Exercise 2.1. Write the addition and multiplication tables for  $\mathbb{Z}/4\mathbb{Z}$

$$\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}.$$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

**Exercise 2.2.** Solve the below equations in  $\mathbb{Z}/7\mathbb{Z}$

i)  $x^2 + \bar{2}x - \bar{1} = \bar{0}$

ii)  $\bar{2}x^2 + \bar{3}x + \bar{2} = \bar{0}$

Sol:  $\mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

use the operation  $\bar{a}\bar{b} = \bar{ab}$   $\bar{a} + \bar{b} = \bar{a+b}$

i)  $x=0 : \bar{0} \cdot \bar{0} + \bar{2} \cdot \bar{0} - \bar{1} = \bar{1}$

$x=1 : \bar{1} \cdot \bar{1} + \bar{2} \cdot \bar{1} - \bar{1} = \bar{2}$

$x=2 : \bar{2} \cdot \bar{2} + \bar{2} \cdot \bar{2} - \bar{1} = \bar{0}$  ✓ solution  $x = \bar{2}$

$x=3 : \bar{3} \cdot \bar{3} + \bar{2} \cdot \bar{3} - \bar{1} = \bar{2} + \bar{6} - \bar{1} = \bar{0}$  ✓ solution  $x = \bar{3}$

$x=4 : \bar{4} \cdot \bar{4} + \bar{2} \cdot \bar{4} - \bar{1} = \bar{2} + \bar{1} \cdot \bar{1} = \bar{2}$

$x=5 : \bar{5} \cdot \bar{5} + \bar{2} \cdot \bar{5} - \bar{1} = \bar{4} + \bar{3} - \bar{1} = \bar{1}$

$x=6 : \bar{6} \cdot \bar{6} + \bar{2} \cdot \bar{6} - \bar{1} = \bar{1} + \bar{5} - \bar{1} = \bar{1}$

ii)  $x=0 : \bar{2} \cdot \bar{0} + \bar{3} \cdot \bar{0} + \bar{2} = \bar{2}$

$x=1 : \bar{2} \cdot \bar{1} + \bar{3} \cdot \bar{1} + \bar{2} = \bar{0}$  ✓ solution  $x = \bar{1}$

$x=2 : \bar{2} \cdot \bar{4} + \bar{3} \cdot \bar{2} + \bar{2} = \bar{2}$

$x=3 : \bar{2} \cdot \bar{2} + \bar{3} \cdot \bar{3} + \bar{2} = \bar{4} + \bar{2} + \bar{2} = \bar{1}$

$x=4 : \bar{2} \cdot \bar{2} + \bar{3} \cdot \bar{4} + \bar{2} = \bar{4} + \bar{5} + \bar{2} = \bar{4}$

$x=5 : \bar{2} \cdot \bar{4} + \bar{3} \cdot \bar{5} + \bar{2} = \bar{1} + \bar{1} + \bar{2} = \bar{4}$

$x=6 : \bar{2} \cdot \bar{1} + \bar{3} \cdot \bar{6} + \bar{2} = \bar{2} + \bar{4} + \bar{2} = \bar{1}$

Thus i) has solution  $x = \bar{2}$  and  $x = \bar{3}$ , ii) has solution  $x = \bar{1}$ .

**Exercise 4.1.** Let  $G$  be a group with operations  $*$ . Prove that  $G$  with respect to the operation  $g_1 * g_2 = g_2 * g_1$  is also a group.

Pf:  $\bullet : G \times G \rightarrow G$ .

1) Closeness. since  $g_1, g_2 \in G$ .  $g_1 * g_2 = g_2 * g_1 \in G$  (since  $*$  is binary operation w.r.t.  $G$ )

2) Associative.  $\forall g_1, g_2, g_3 \in G$ .  $g_1 \cdot (g_2 \cdot g_3) = g_1 \cdot (g_3 * g_2) = (g_3 * g_2) * g_1$ . (by def. of operation  $\bullet$ )  
 $= g_3 * (g_2 * g_1)$  (by associativity of  $*$ )  
 $= (g_2 * g_1) \cdot g_3$ .  $= (g_1 \cdot g_2) \cdot g_3$  (by def. operation  $\bullet$ )

3)  $\exists e \in G$ , which is the identity element of operation  $*$ .  $\forall g_1 \in G$

$e * g_1 = g_1 * e = g_1$ .  $g_1 * e = e * g_1 = e$

which shows  $e$  is also an identity element of operation  $\bullet$ .

4)  $\forall g_1 \in G$ .  $\exists g'_1$  s.t.  $g_1 * g'_1 = g'_1 * g_1 = e$  (since  $G$  is a group w.r.t.  $*$ )

$g_1 * g'_1 = g'_1 * g_1 = e$   $g'_1 * g_1 = g_1 * g'_1 = e$  thus the inverse exists for any elements in  $G$  w.r.t. operation  $\bullet$ .

In conclusion.  $G$  w.r.t. operation  $\bullet$  is also a group.

**Exercise 4.2.** Show that the set of functions  $f(t) = \frac{at+b}{ct+d}$  where  $a, b, c, d \in \mathbb{R}$ ,  $ad - bc \neq 0$  is a group with respect to composition.

Sol: denote that the group  $F = \{f(t) \mid f(t) = \frac{at+b}{ct+d}, a, b, c, d \in \mathbb{R}, ad - bc \neq 0\}$ .

$$\forall f_1(t) = \frac{a_1t+b_1}{c_1t+d_1} \quad f_2(t) = \frac{a_2t+b_2}{c_2t+d_2} \in F.$$

$$1) f_1(f_2(t)) = \frac{(a_1a_2 + b_1c_2)t + (a_1b_2 + b_1d_2)}{(c_1a_2 + d_1c_2)t + (c_1b_2 + d_1d_2)}$$

$$(a_1a_2 + b_1c_2)(c_1b_2 + d_1d_2) - (c_1a_2 + d_1c_2)(a_1b_2 + b_1d_2) = a_1a_2d_1d_2 + b_1b_2c_1c_2 - a_2b_1c_1d_2 - a_1c_2b_2d_1$$

$$= a_1d_1(a_2d_2 - c_2d_2) + b_1c_1(b_2c_2 - a_2d_2) = (a_1d_1 - c_1b_1)(a_2d_2 - c_2b_2) \neq 0. \text{ operation is closed.}$$

2) the composition is associative by the def. of composition

3)  $\exists e(t) = t$ . ( $a=1, c=0, b=0, d=1$ ) identity element.

$$f(e(t)) = e(f(t)) = \frac{at+b}{ct+d}$$

$$4) \forall f = \frac{at+b}{ct+d} \in F.$$

$$\exists f^{-1} = \frac{dt-b}{-ct+a} \in F. \text{ s.t. } f^{-1}(f(t)) = \frac{d(\frac{at+b}{ct+d}) - b}{-c(\frac{at+b}{ct+d}) + a} = \frac{dat - cbt}{-cb + ad} = t. \text{ similarly } f(f^{-1}(t)) = t.$$

thus, all elements are invertible.

**Exercise 4.3.** Which of the below subsets of  $\mathbb{Z}/10\mathbb{Z}$  form groups with respect to multiplication?

- i)  $\{\bar{1}, \bar{9}\}$
- ii)  $\{\bar{1}, \bar{7}\}$
- iii)  $\{\bar{1}, \bar{3}, \bar{7}\}$
- iv)  $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

Remark. In what follows the symbol \* will be often omitted in the notation of the group operation (juxtaposition).

Sol: denote the set be  $A_1, A_2, A_3, A_4$ . by prop. 2.3.2.  $\bar{1}$  is the identity element.

(1)  $A_1$  is a group.

① operation is closed.  $\bar{1} \cdot \bar{1} = \bar{1} \in A_1, \bar{1} \cdot \bar{9} = \bar{9} \in A_1, \bar{9} \cdot \bar{9} = \bar{1} \in A_1,$

② by prop. 2.3. the multiplication in  $\mathbb{Z}/m\mathbb{Z}$  is associative

③  $\bar{1}$  is identity element  $\bar{1} \cdot \bar{9} = \bar{9} \cdot \bar{1} = \bar{9} \quad \bar{1} \cdot \bar{1} = \bar{1} \cdot \bar{1} = \bar{1}$

④  $\bar{9}$  has inverse  $\bar{9} \quad \bar{9}$  has inverse  $\bar{1}$

(2)  $A_2$  not group.

for  $\bar{7} \in A_2 \quad \bar{7} \cdot \bar{7} = \bar{9} \quad \bar{7} \cdot \bar{1} = \bar{7}$ . i.e.  $\bar{7}$  do not have inverse

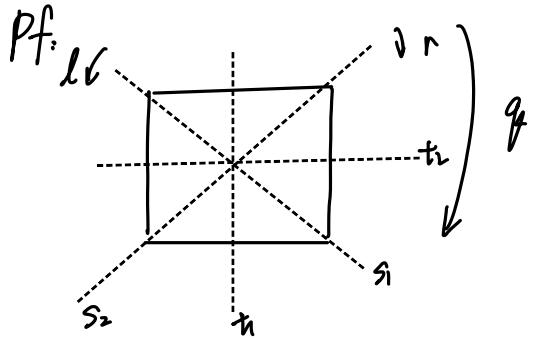
(3).  $A_3$  not a group

the operation is not closed since  $\bar{3} \cdot \bar{3} = \bar{9} \notin A_3$ .

(4)  $A_4$  not a group.

same as (3)

**Exercise 4.4.** Draw the Cayley table of the group  $D_4$ . Consider a square with center  $O$ . Let  $e$  be the identity map,  $r$  is the clockwise rotation about  $O$  by  $90^\circ$ ,  $l$  is the counterclockwise rotation about  $O$  by  $90^\circ$ ,  $q$  be the rotation about  $O$  by  $180^\circ$  (= a point reflection),  $s_1, s_2$  be the reflections across the diagonals,  $t_1, t_2$  be the reflections across the lines connecting the midpoints of the opposite edges. Then  $D_4 = \{e, r, l, q, t_1, t_2, s_1, s_2\}$ .



	$e$	$r$	$l$	$q$	$t_1$	$t_2$	$s_1$	$s_2$
$e$	$e$	$r$	$l$	$q$	$t_1$	$t_2$	$s_1$	$s_2$
$r$	$r$	$q$	$e$	$l$	$s_2$	$s_1$	$t_1$	$t_2$
$l$	$l$	$e$	$q$	$r$	$s_1$	$s_2$	$t_2$	$t_1$
$q$	$q$	$l$	$r$	$e$	$t_2$	$t_1$	$s_2$	$s_1$
$t_1$	$t_1$	$s_1$	$s_2$	$t_2$	$e$	$q$	$r$	$l$
$t_2$	$t_2$	$s_2$	$s_1$	$t_1$	$q$	$e$	$l$	$r$
$s_1$	$s_1$	$t_2$	$t_1$	$s_2$	$l$	$r$	$e$	$q$
$s_2$	$s_2$	$t_1$	$t_2$	$s_1$	$r$	$l$	$q$	$e$

$A \begin{matrix} B \\ D \end{matrix} \xrightarrow{t_1} B \begin{matrix} A \\ C \end{matrix} \xrightarrow{r} C \begin{matrix} B \\ D \end{matrix} \xrightarrow{t_2} D \begin{matrix} A \\ C \end{matrix} \xrightarrow{l} A \begin{matrix} D \\ B \end{matrix} \xrightarrow{q} B \begin{matrix} C \\ A \end{matrix} \xrightarrow{s_1} C \begin{matrix} D \\ B \end{matrix} \xrightarrow{s_2} D \begin{matrix} A \\ C \end{matrix}$	$B \begin{matrix} C \\ D \end{matrix} \xrightarrow{t_1} C \begin{matrix} D \\ A \end{matrix} \xrightarrow{r} D \begin{matrix} A \\ B \end{matrix} \xrightarrow{t_2} A \begin{matrix} B \\ C \end{matrix} \xrightarrow{l} B \begin{matrix} C \\ D \end{matrix} \xrightarrow{q} C \begin{matrix} A \\ B \end{matrix} \xrightarrow{s_1} D \begin{matrix} B \\ A \end{matrix} \xrightarrow{s_2} A \begin{matrix} C \\ D \end{matrix}$	$C \begin{matrix} D \\ A \end{matrix} \xrightarrow{t_1} D \begin{matrix} A \\ B \end{matrix} \xrightarrow{r} A \begin{matrix} B \\ C \end{matrix} \xrightarrow{t_2} B \begin{matrix} C \\ D \end{matrix} \xrightarrow{l} C \begin{matrix} D \\ A \end{matrix} \xrightarrow{q} D \begin{matrix} B \\ C \end{matrix} \xrightarrow{s_1} A \begin{matrix} C \\ D \end{matrix} \xrightarrow{s_2} B \begin{matrix} A \\ C \end{matrix}$
$A \begin{matrix} B \\ D \end{matrix} \xrightarrow{r} D \begin{matrix} A \\ C \end{matrix} \xrightarrow{t_1} A \begin{matrix} D \\ B \end{matrix} \xrightarrow{t_2} C \begin{matrix} B \\ A \end{matrix} \xrightarrow{s_1} D \begin{matrix} C \\ B \end{matrix} \xrightarrow{s_2} B \begin{matrix} A \\ D \end{matrix}$	$B \begin{matrix} C \\ D \end{matrix} \xrightarrow{r} D \begin{matrix} B \\ A \end{matrix} \xrightarrow{t_1} C \begin{matrix} A \\ D \end{matrix} \xrightarrow{t_2} A \begin{matrix} D \\ B \end{matrix} \xrightarrow{s_1} B \begin{matrix} C \\ A \end{matrix} \xrightarrow{s_2} D \begin{matrix} B \\ C \end{matrix}$	$C \begin{matrix} D \\ A \end{matrix} \xrightarrow{r} A \begin{matrix} B \\ D \end{matrix} \xrightarrow{t_1} B \begin{matrix} C \\ A \end{matrix} \xrightarrow{t_2} D \begin{matrix} A \\ C \end{matrix} \xrightarrow{s_1} C \begin{matrix} B \\ D \end{matrix} \xrightarrow{s_2} A \begin{matrix} D \\ B \end{matrix}$
$A \begin{matrix} B \\ D \end{matrix} \xrightarrow{r} C \begin{matrix} D \\ B \end{matrix} \xrightarrow{t_1} A \begin{matrix} D \\ B \end{matrix} \xrightarrow{t_2} C \begin{matrix} B \\ D \end{matrix} \xrightarrow{s_1} D \begin{matrix} C \\ B \end{matrix} \xrightarrow{s_2} B \begin{matrix} A \\ D \end{matrix}$	$B \begin{matrix} C \\ D \end{matrix} \xrightarrow{r} A \begin{matrix} D \\ B \end{matrix} \xrightarrow{t_1} C \begin{matrix} A \\ D \end{matrix} \xrightarrow{t_2} B \begin{matrix} C \\ A \end{matrix} \xrightarrow{s_1} D \begin{matrix} B \\ C \end{matrix} \xrightarrow{s_2} A \begin{matrix} D \\ B \end{matrix}$	$C \begin{matrix} D \\ A \end{matrix} \xrightarrow{r} B \begin{matrix} A \\ D \end{matrix} \xrightarrow{t_1} D \begin{matrix} C \\ B \end{matrix} \xrightarrow{t_2} A \begin{matrix} B \\ C \end{matrix} \xrightarrow{s_1} C \begin{matrix} D \\ A \end{matrix} \xrightarrow{s_2} B \begin{matrix} A \\ D \end{matrix}$

Exercise 4.5. Are the below tables the Cayley tables of certain groups?

	2	0	1	3	↓
a	a	b	c	d	暂时对应 (Z/4Z,+)
b	b	a	d	c	
c	d	c	a	b	
d	c	d	b	a	

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

$$(1) A = \{a, b, c, d\}$$

① the operation is closed.

② b is the identity elements.

③  $b * b = b$     $a * a = a * a = b$ .    $c * d = d * c = b$ . all elements has inverse.

④ i) if one of  $e_1 = b$ , the associative is easy to check

since  $(e_1 * b) * e_2 = e_1 * e_2 = e_1 * (b * e_2)$  or  $b * (e_1 * e_2) = e_1 * e_2 = (b * e_1) * e_2$

ii) the table is symmetric, thus the operation is commutative.

iii)  $\forall e_1, e_2, e_3 \in G$ . we have  $e_1 * (e_2 * e_3) = e_1 * (e_3 * e_2) = (e_3 * e_2) * e_1 = (e_2 * e_3) * e_1$

$(e_1 * e_2) * e_3 = (e_2 * e_1) * e_3 = e_3 * (e_1 * e_2) = e_3 * (e_2 * e_1)$

$e_2 * (e_1 * e_3) = (e_1 * e_3) * e_2 = e_2 * (e_3 * e_1) = (e_3 * e_1) * e_2$

thus if we can prove  $e_1 * (e_2 * e_3) = (e_1 * e_2) * e_3$  then we have  $(e_1 * e_2) * e_3 = (e_2 * e_1) * e_3 = e_2 * (e_1 * e_3)$

i.e. the 12 operation above are equal. the associativity holds for any associative with  $e_1, e_2, e_3$

iv) for the case  $e_1 = e_2 = e_3$ .  $e_1 * (e_1 * e_1) = (e_1 * e_1) * e_1$  by commutative.

v) check the remaining case:

$$\begin{cases} (a * c) * d = d * d = a \\ a * (c * d) = a * b = a. \end{cases} \quad \begin{cases} (a * a) * d = b * d = d \\ a * (a * d) = a * c = d \end{cases} \quad \begin{cases} (a * a) * c = b * c = c \\ a * (a * c) = a * d = c \end{cases} \quad \begin{cases} (c * c) * d = a * d = c \\ c * (c * d) = c * b = c \end{cases}$$

$$\begin{cases} (c * c) * a = a * a = b \\ c * (c * a) = c * d = b. \end{cases} \quad \begin{cases} (d * d) * a = a * a = b \\ d * (d * a) = d * c = b \end{cases} \quad \begin{cases} (d * d) * c = a * c = d \\ d * (d * c) = d * b = d. \end{cases}$$

thus, the operation is associative.

$$(2) B = \{a, b, c, d, e\}. \text{ not Cayley table.}$$

① the operation is closed.

② e is the identity elements.

③ every element itself is the inverse.

④  $(b * b) * d = e * d = d$  so the operation is not associative.

$$b * (b * d) = b * c = a.$$

**Exercise 5.1.** Prove that the orthogonal matrices  $\{A \in M_n(\mathbb{R}) \mid AA^T = E_n\}$  form a subgroup of  $GL_n(\mathbb{R})$ .

Pf: denote  $H = \{A \in M_n(\mathbb{R}) \mid AA^T = E_n\}$

$$(1) \forall A_1, A_2 \in H \quad A_2 A_2^T = A_1 A_1^T = E_n.$$

$$A_1 A_2 (A_1 A_2)^T = A_1 A_2 A_2^T A_1^T = A_1 E_n A_1^T = E_n. \text{ thus } A_1 A_2 \in H$$

$$(2) \forall A \in H. \quad A^{-1} = A^T$$

$$A^T \cdot (A^T)^T = A^T \cdot A = A^{-1} \cdot A = E_n, \text{ thus } A^T \in H.$$

**Exercise 5.2.** Let  $G, G'$  be groups and  $H < G, H' < G'$ . Show that  $H \times H' < G \times G'$ .

$$1). \forall (h_1, h'_1), (h_2, h'_2) \in H \times H'$$

$$(h_1, h'_1) \cdot (h_2, h'_2) = (h_1 * h_2, h'_1 * h'_2)$$

since  $H, H'$  are subgroup.  $h_1 * h_2 \in H. h'_1 * h'_2 \in H'$ . thus.  $(h_1, h'_1) \cdot (h_2, h'_2) \in H \times H'$

$$2). \forall (h, h') \in H \times H'$$

since  $H, H'$  are subgroup.  $\exists h^{-1} \in H. h'^{-1} \in H'$  s.t.  $h * h^{-1} = h'^{-1} * h = e. h' * h'^{-1} = h'^{-1} * h' = e$

$$\text{thus } \exists (h, h')^{-1} = (h^{-1}, h'^{-1}) \in H \times H' \text{ s.t. } (h, h') \cdot (h^{-1}, h'^{-1}) = (h^{-1}, h'^{-1}) \cdot (h, h') = (e, e')$$

**Exercise 5.3.** Find all the non-trivial subgroups of  $\mathbb{Z}/6\mathbb{Z}$ .

$$A = \{\bar{0}, \bar{2}, \bar{4}\} \quad B = \{\bar{0}, \bar{3}\} \text{ are subgroups.}$$

$$(1) \bar{0} + \bar{2} = \bar{2} \quad \bar{0} + \bar{4} = \bar{4} \quad \bar{2} + \bar{4} = \bar{0} \quad \bar{0} + \bar{0} = \bar{0} \quad \bar{2} + \bar{2} = \bar{4} \quad \bar{4} + \bar{4} = \bar{2} \quad \in A.$$

$\bar{0}$  has inverse  $\bar{0}$ .  $\bar{3}$  has inverse  $\bar{4}$ .

$$(2) \bar{0} + \bar{3} = \bar{3}. \quad \bar{0} + \bar{0} = \bar{0} \quad \bar{3} + \bar{3} = \bar{0}$$

$\bar{0}$  has inverse  $\bar{0}$ .  $\bar{3}$  has inverse  $\bar{3}$ .

Assume there is another subgroup.  $H \subseteq \mathbb{Z}/6\mathbb{Z}$ .

$\bar{0}$ . identity element must contain in  $H$ .

if  $\bar{1} \in H$ . then  $\bar{H} = \mathbb{Z}/6\mathbb{Z}$ . since  $\bar{1} + \bar{1} = \bar{2}. \bar{1} + \bar{2} = \bar{3}. \bar{1} + \bar{3} = \bar{4}. \bar{1} + \bar{4} = \bar{5} \dots$

if  $\bar{2} \in H$ . then we have  $A \subseteq H$ .

if  $\bar{3} \in H$ . then we have  $B \subseteq H$ .

if  $\bar{4} \in H$ . then  $\bar{4} + \bar{4} = \bar{2}$ .  $A \subseteq H$ .

if  $\bar{5} \in H$  then  $\bar{5} + \bar{5} = \bar{0}. \bar{4} + \bar{5} = \bar{3}. \bar{5} + \bar{3} = \bar{2}. \bar{5} + \bar{2} = \bar{1}$ .  $H = \mathbb{Z}/6\mathbb{Z}$ .

and if  $\bar{2}, \bar{3}, \bar{4} \in H$  simultaneously,  $\bar{3} + \bar{4} = \bar{1}. \bar{3} + \bar{2} = \bar{5}$ .  $H = \mathbb{Z}/6\mathbb{Z}$

thus, no other subgroup except  $\{\bar{0}, \bar{2}, \bar{4}\}, \{\bar{0}, \bar{3}\}$

Exercise 5.4. Prove that the only finite subgroup of  $\mathbb{R}^*$  is  $\{\pm 1\}$ . nontrivial.

Pf:  $(\mathbb{R}^*, \{0\}, \times)$

Assume the converse there exist nontrivial finite subgroup.  $H = \{a_1, \dots, a_n\}$ .

if one of  $|a_i| > 1$ .  $\lim_{m \rightarrow \infty} |a_i|^m = +\infty$  there must exist sequence  $\{a_i, a_i^2, a_i^3, \dots, a_i^m, \dots\} \subseteq H$

which contains infinite many elements.

if  $|a_i| < 1$ . its inverse  $|a_i^{-1}| > 1$  and  $a_i^{-1} \in H$  by def. of subgroup.

thus the only possible case is  $|a_i| = 1$ . i.e. only nontrivial subgroup is  $\{\pm 1\}$ .

Exercise 5.5. Find all the non-trivial subgroups of  $D_4$ .

Sol: we use the Cayley table which we find in Ex 4.4

	e	r	t	q	$t_1$	$t_2$	$s_1$	$s_2$
e	e	r	t	q	$t_1$	$t_2$	$s_1$	$s_2$
r	r	q	e	t	$s_2$	$s_1$	$t_1$	$t_2$
t	t	e	q	r	$s_1$	$s_2$	$t_2$	$t_1$
q	q	t	r	e	$t_2$	$t_1$	$s_2$	$s_1$
$t_1$	$t_1$	$s_1$	$s_2$	$t_2$	e	q	$r$	$t$
$t_2$	$t_2$	$s_2$	$s_1$	$t_1$	q	e	$t$	$r$
$s_1$	$s_1$	$t_2$	$t_1$	$s_2$	$t$	$r$	e	q
$s_2$	$s_2$	$t_1$	$t_2$	$s_1$	$r$	$t$	q	e

by the table

$\{e, r, t, q\} \rightarrow$  block the table.

$\{t_1, e\}, \{t_2, e\}, \{s_1, e\}, \{s_2, e\}, \{q, e\}, \{t_1, t_2, e, q\}, \{s_1, s_2, e, q\}$

	e	r	t	q	$t_1$	$t_2$	$s_1$	$s_2$
e	e	r	t	q	$t_1$	$t_2$	$s_1$	$s_2$
r	r	q	e	t	$s_2$	$s_1$	$t_1$	$t_2$
t	t	e	q	r	$s_1$	$s_2$	$t_2$	$t_1$
q	q	t	r	e	$t_2$	$t_1$	$s_2$	$s_1$
$t_1$	$t_1$	$s_1$	$s_2$	$t_2$	e	q	$r$	$t$
$t_2$	$t_2$	$s_2$	$s_1$	$t_1$	q	e	$t$	$r$
$s_1$	$s_1$	$t_2$	$t_1$	$s_2$	$r$	$t$	e	q
$s_2$	$s_2$	$t_1$	$t_2$	$s_1$	$t$	$r$	q	e

	e	r	t	q	$t_1$	$t_2$	$s_1$	$s_2$
e	e	r	t	q	$t_1$	$t_2$	$s_1$	$s_2$
r	r	q	e	t	$s_2$	$s_1$	$t_1$	$t_2$
t	t	e	q	r	$s_1$	$s_2$	$t_2$	$t_1$
q	q	t	r	e	$t_2$	$t_1$	$s_2$	$s_1$
$t_1$	$t_1$	$s_1$	$s_2$	$t_2$	e	q	$r$	$t$
$t_2$	$t_2$	$s_2$	$s_1$	$t_1$	q	e	$t$	$r$
$s_1$	$s_1$	$t_2$	$t_1$	$s_2$	$r$	$t$	e	q
$s_2$	$s_2$	$t_1$	$t_2$	$s_1$	$t$	$r$	q	e

cross out some row/ column directly shows the closeness  
invertibility also is obtained directly by observing the table.

Exercise 6.1. Let  $G$  be a group and  $g, h \in G$ . Show that  $\text{ord } gh = \text{ord } hg$ .

Pf: denote  $\text{ord } gh = m$ .

1) if  $m$  be finite.  $(gh)^m = e$   $\underbrace{(g * h) * (g * h) * \dots * (g * h)}_{m \text{ times}} = e$

thus  $m \geq \text{ord } hg$ .

$\Rightarrow g * (h * g)^{m-1} * h = e$ . by associativity of operation in group.

↑

$\Rightarrow$  pre-multi  $g^{-1}$ . post-multi  $h^{-1}$ .  $(hg)^{m-1} = g^{-1} \cdot h^{-1} \Rightarrow (hg)^{m-1} = (hg)^{-1} \Rightarrow (hg)^m = e$ .  
prop. 1.4.

thus  $\text{ord } hg = \text{ord } gh = m$ .

$(gh)^n = e$ . i-  $(hg)^m = e \Rightarrow (gh)^m = e \Rightarrow m \geq n$ .

then  $(gh)^n = e \Rightarrow (hg)^n = e \Rightarrow m = n$ .

assume the converse.  $\exists n \in \mathbb{N}$ .  $(hg)^n = e$ , similarly in 1). we have  $(gh)^n = e$ . contradicts.

thus.  $\text{ord } hg = +\infty$ .

**Exercise 6.2.** Show that  $\text{ord } g^s = n/d$  where  $n = \text{ord } g, d = \gcd(n, s)$ .

*Hint.* Use Proposition 6.3.

Pf: first assume all the numbers here are finite. otherwise there is nothing to prove.

$$\begin{aligned} (g^s)^{\frac{n}{d}} &= g^{\frac{ns}{d}} \quad (\text{by prop. 6.1}) \\ &= (g^n)^{\frac{s}{d}} \quad (\text{by prop. 6.1}) \\ &= e^{\frac{s}{d}} = e. \quad (\text{since. } d = \gcd(n, s). \quad d \mid s. \quad \frac{s}{d} \in \mathbb{Z}.) \end{aligned}$$

then shows.  $\frac{n}{d}$  the least element. satisfy that condition.

$$\text{assume } \exists A < \frac{n}{d} \quad (g^s)^A = e. \Rightarrow$$

by prop. 6.3. we have  $A \cdot \frac{n}{d} \Rightarrow A t_1 = \frac{n}{d}$  for some integer  $t_1 \neq 1$ .

Since  $n = \text{ord } g$  and  $g^{SA} = e$ , again by prop 6.3.  $n \mid SA$ .

thus  $SA = t_1 n$  for some integer  $t_1 \neq 1$ . i.e.  $A = \frac{t_1 n}{s}$ .

$$\begin{cases} A = \frac{t_1 n}{s} \\ A t_1 = \frac{n}{d} \end{cases} \Rightarrow \frac{t_1 n}{s} = \frac{n}{t_1 d} \Rightarrow s = t_1 t_2 d. \quad \text{that is. } \begin{cases} n = t_1 d \\ s = t_1 d t_2 \end{cases} \quad \text{we have } t_1 d > d$$

which contradicts to  $d = \gcd(s, n)$ . Thus.  $\text{ord } g^s = \frac{n}{d}$

**Exercise 7.1.** Find the left and the right cosets for

- i)  $G = D_4, H = \{e, s_1\}$
- ii)  $G = D_4, H = \{e, t_1\}$
- iii)  $G = D_4, H = \{e, q\}$

	e	r	l	q	$t_1$	$t_2$	$s_1$	$s_2$
e	e	r	l	q	$t_1$	$t_2$	$s_1$	$s_2$
r	r	q	e	l	$s_2$	$s_1$	$t_1$	$t_2$
l	l	e	q	r	$s_1$	$s_2$	$t_2$	$t_1$
q	q	l	r	e	$t_2$	$t_1$	$s_2$	$s_1$
$t_1$	$t_1$	$s_1$	$s_2$	$t_2$	e	q	r	l
$t_2$	$t_2$	$s_2$	$s_1$	$t_1$	q	e	l	r
$s_1$	$s_1$	$t_2$	$t_1$	$s_2$	l	r	e	q
$s_2$	$s_2$	$t_1$	$t_2$	$s_1$	r	l	q	e

Pf: by the previous table.

i) left coset :  $eH = s_1 H = \{e, s_1\}$ .

right coset

$$He = HS_1 = \{e, s_1\}$$

$$rH = t_1 H = \{re, rs_1\} = \{r, t_1\}.$$

$$Hr = Ht_2 = \{er, sr\} = \{r, t_2\}$$

$$lH = t_2 H = \{le, lt_1\} = \{l, t_2\}$$

$$Hl = Ht_1 = \{el, sr\} = \{l, t_1\}$$

$$qH = s_2 H = \{q, s_2\}.$$

$$HQ = HS_2 = \{eq, s_1 q\} = \{q, s_2\}$$

ii) left coset.  $eH = t_1 H = \{e, t_1\}$

right coset

$$He = Ht_1 = \{e, t_1\}$$

$$rH = s_2 H = \{re, rt_1\} = \{r, s_2\}$$

$$Hr = HS_1 = \{r, s_1\}$$

$$lH = s_1 H = \{le, lt_1\} = \{l, s_1\}$$

$$Hl = HS_2 = \{l, s_2\}$$

$$qH = t_2 H = \{q, t_2\}$$

$$HQ = Ht_2 = \{q, t_2\}$$

iii) left coset:  $eH = qH = \{e, q\}$ .

right coset

$$He = HQ = \{e, q\}.$$

$$rH = lH = \{r, l\}.$$

$$Hr = Hl = \{r, l\}$$

$$t_1 H = t_2 H = \{t_1, t_2\}$$

$$Ht_1 = Ht_2 = \{t_1, t_2\}$$

$$s_1 H = s_2 H = \{s_1, s_2\}.$$

$$HS_1 = HS_2 = \{s_1, s_2\}$$

# Homework 3. Week 12th

Exercise 7.2. Prove that  $\{A \in \mathrm{GL}_n(\mathbb{C}) \mid \det A \in \mathbb{R}\}$  is a normal subgroup of  $\mathrm{GL}_n(\mathbb{C})$ .

Pf: denote  $H = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid \det A \in \mathbb{R}\}$ .

1)  $H$  is a subgroup

$$\forall A, B \in H \quad \det AB = \det A \cdot \det B \in \mathbb{R}.$$

$$\forall A \in H \quad \det A^{-1} = \frac{1}{\det A} \in \mathbb{R}.$$

2)  $H$  is normal

$$\forall A \in \mathrm{GL}_n(\mathbb{C}). \text{ if } A \in H, \text{ then } AH = HA = H.$$

if  $A \in \mathrm{GL}_n(\mathbb{C}) \setminus H$ . i.e.  $\det A \in \mathbb{C} \setminus \mathbb{R}$ .

$$\forall B \in H. \quad \det AB = \det A \cdot \det B.$$

$$\det BA = \det B \cdot \det A.$$

thus  $AH = HA$ , the codomain of the determinant is.  $\{\det A \cdot \mathbb{R}\}$ .

In conclusion.  $H$  is a normal subgroup.

Exercise 7.3. Prove that the intersection of two normal subgroups is a normal subgroup.

Pf: denote  $H_1, H_2$  - normal subgroup of  $G$ . with operation  $*$ .

by lemma 5.3.  $H = H_1 \cap H_2$  is subgroup.

$$\forall g \in G. \quad \forall h \in H.$$

since  $h \in H \subseteq H_1$ .  $H_1$  is normal.  $gH_1 = H_1g$ .  $hg \in gH_1$

since  $h \in H \subseteq H_2$ .  $H_2$  is normal.  $gH_2 = H_2g$ .  $hg \in gH_2$   $\Rightarrow hg \in gH$ .

since  $h$  is arbitrary.  $Hg \subseteq gH$ . similarly,  $Hg \supseteq gH$ . thus  $gH = Hg$

since  $g$  is arbitrary.  $H$  is normal subgroup of  $G$ .

Exercise 7.4. Let  $n \geq 3$  and  $1 \leq m \leq n$ . Prove that  $\{\sigma \in S_n \mid \sigma(m) = m\}$  is not a normal subgroup of  $S_n$ .

Pf: denote  $H_n^m = \{\sigma \in S_n \mid \sigma(m) = m\}$ .

$$\text{let } n=3. \quad H_3^2 = \{(123), (321)\}$$

$$\text{let } g = (213). \quad gH_3^2 = \{(231), (132)\} \quad H_3^2g = \{(123), (231)\}$$

$$gH_3^2 \neq H_3^2g.$$

Exercise 7.5. Let  $G$  be a group and  $g_1 \sim g_2, g_1, g_2 \in G$  if  $g_1$  is a conjugate of  $g_2$ .

- Prove that the relation  $\sim$  on  $G$  is an equivalence relation
- Find the partition of  $G = D_3, D_4$  into the equivalence classes

Pf: i) ①  $\exists g = e$ .  $eg, e^{-1} = g$ , for any  $g \in G$ . thus  $g_1 \sim g_1$

②  $g_1 \sim g_2 \Rightarrow \exists g \in G$ .  $gg_2g^{-1} = g_1 \Rightarrow g_1 = g^{-1}g_2g$

, since  $G$  is a group.  $g^{-1} \in G$  and  $(g^{-1})^{-1} = g$ .  $g_2 \sim g_1$ .

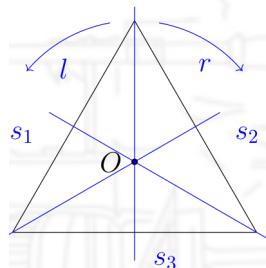
③  $g_1 \sim g_2, g_2 \sim g_3 \Rightarrow \exists g, h \in G$ .  $g_1 = gg_2g^{-1}, g_2 = hg_3h^{-1}$

$\Rightarrow g_1 = (gh)g_3h^{-1}g^{-1}$  since  $G$  is a group.  $gh \in G$ .  $h^{-1}g^{-1} = (gh)^{-1} \in G$ . thus  $g_1 \sim g_3$ .

ii) for  $D_3$ , we have the table.

$$\{r, l\} \quad r \cdot l \cdot r^{-1} = r \cdot l \cdot l = e \cdot l = l \quad r \sim l.$$

	$e$	$l$	$r$	$s_1$	$s_2$	$s_3$
$e$	$e$	$l$	$r$	$s_1$	$s_2$	$s_3$
$l$	$l$	$r$	$e$	$s_2$	$s_3$	$s_1$
$r$	$r$	$e$	$l$	$s_3$	$s_1$	$s_2$
$s_1$	$s_1$	$s_3$	$s_2$	$e$	$r$	$l$
$s_2$	$s_2$	$s_1$	$s_3$	$l$	$e$	$r$
$s_3$	$s_3$	$s_2$	$s_1$	$r$	$l$	$e$



$$\{s_1, s_2, s_3\} \quad s_1 s_2 s_1^{-1} = s_1 s_2 s_1 = r s_1 = s_3 \quad s_1 \sim s_3.$$

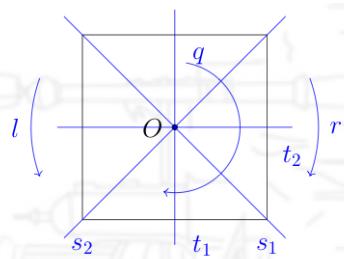
$$s_1 s_3 s_1^{-1} = s_1 s_3 s_1 = l s_1 = s_2 \quad s_2 \sim s_3.$$

$$\{e\}. \quad \forall h \in D_3. \quad h \cdot h^{-1} = h \cdot h^{-1} = e.$$

3 equivalent classes  $\{r, l\}$   $\{s_1, s_2, s_3\}$ .  $\{e\}$ .

for  $D_4$ , we have the table.

	$e$	$r$	$l$	$q$	$t_1$	$t_2$	$s_1$	$s_2$
$e$	$e$	$r$	$l$	$q$	$t_1$	$t_2$	$s_1$	$s_2$
$r$	$r$	$q$	$e$	$l$	$s_2$	$s_1$	$t_1$	$t_2$
$l$	$l$	$e$	$q$	$r$	$s_1$	$s_2$	$t_2$	$t_1$
$q$	$q$	$l$	$r$	$e$	$t_2$	$t_1$	$s_2$	$s_1$
$t_1$	$t_1$	$s_1$	$s_2$	$t_2$	$e$	$q$	$r$	$l$
$t_2$	$t_2$	$s_2$	$s_1$	$t_1$	$q$	$e$	$l$	$r$
$s_1$	$s_1$	$t_2$	$t_1$	$s_2$	$l$	$r$	$e$	$q$
$s_2$	$s_2$	$t_1$	$t_2$	$s_1$	$r$	$l$	$q$	$e$



$$r \cdot l \cdot r^{-1} = q \cdot l = r \quad l \sim r.$$

$$l \cdot q \cdot l^{-1} = r \cdot r = q. \quad s_1 \cdot q \cdot s_1^{-1} = s_2 \cdot s_1 = q.$$

$$r \cdot s_2 \cdot r^{-1} = t_2 \cdot l = s_1 \quad s_1 \sim s_2.$$

$$l \cdot t_1 \cdot l^{-1} = s_1 \cdot r = t_2 \quad t_1 \sim s_2.$$

5 equivalent class.  $\{r, l\}$ ,  $\{s_1, s_2\}$ ,  $\{t_1, t_2\}$ ,  $\{e\}$ ,  $\{q\}$ .

Exercise 8.1. Let  $H_1, H_2$  be subgroups of a finite group  $G$  and  $|H_1| = 15, |H_2| = 28$ .

- Find the minimum possible order of  $G$ .

- Prove that  $H_1 \cap H_2 = \{e\}$ .

i) by Lagrange thm.

possible minimum order =  $\text{lcm}(15, 28) = 420$ .

ii) by lemma 5.3.  $H_1 \cap H_2 = H$  is a subgroup.

We have  $H$  is a subgroup of  $H_1$  and  $H_2$ .

by Lagrange thm.  $|H| = |H| \cdot |H_1 : H|$

$$|H| = |H| \cdot |H : H|.$$

since  $\gcd(|H_1|, |H_2|) = 1$ . we have  $|H| = 1$ . i.e  $H = \{e\}$ .

**Exercise 9.1.** Consider the group  $G = \{ax \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\} \cup \{a/x \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\}$  with respect to composition ( $|G| = 24$ ) and its subgroups  $H = \{\bar{x}, \bar{3x}, \bar{9x}\}$ ,  $H' = \{\pm x, \pm \bar{3}/x\}$ .

- i) Find the left cosets of  $H$
- ii) Show that  $H \triangleleft G$
- iii) Show that  $H'$  is not normal
- iv) Draw the Cayley table of  $G/H$

$$\begin{aligned}(ax) \cdot (bx) &= abx \\(ax) \cdot (b/x) &= ab/x \\(a/x) \cdot (b/x) &= ab^{-1}x \\(a/x) \cdot (b/x) &= ab^{-1}/x.\end{aligned}$$

i).  $\bar{2}x \cdot H = \bar{6}x \cdot H = \bar{5}x \cdot H = \{\bar{2}x, \bar{5}x, \bar{6}x\}$

$\bar{4}x \cdot H = \bar{12}x \cdot H = \bar{10}x \cdot H = \{\bar{4}x, \bar{10}x, \bar{12}x\}$

$\bar{7}x \cdot H = \bar{8}x \cdot H = \bar{11}x \cdot H = \{\bar{7}x, \bar{8}x, \bar{11}x\}$

$x \cdot H = \bar{3}x \cdot H = \bar{9}x \cdot H = \{x, \bar{3}x, \bar{9}x\}$

$x^{-1} \cdot H = \bar{3}x^{-1} \cdot H = \bar{9}x^{-1} \cdot H = \{x^{-1}, \bar{3}x^{-1}, \bar{9}x^{-1}\}$

$\bar{2}x^{-1} \cdot H = \bar{6}x^{-1} \cdot H = \bar{5}x^{-1} \cdot H = \{\bar{2}x^{-1}, \bar{5}x^{-1}, \bar{6}x^{-1}\}$

$\bar{4}x^{-1} \cdot H = \bar{12}x^{-1} \cdot H = \bar{10}x^{-1} \cdot H = \{\bar{4}x^{-1}, \bar{10}x^{-1}, \bar{12}x^{-1}\}$

$\bar{7}x^{-1} \cdot H = \bar{8}x^{-1} \cdot H = \bar{11}x^{-1} \cdot H = \{\bar{7}x^{-1}, \bar{8}x^{-1}, \bar{11}x^{-1}\}$

ii).  $\forall g_1 = \{a_1 x^\alpha \mid a_1 \in (\mathbb{Z}/13\mathbb{Z})^*, \alpha \in \{-1, 1\}\}$

$\alpha = 1, Hg_1 = \{a_1 x, \bar{3} \cdot a_1 x, \bar{9} \cdot a_1 x\}$

this "composition" is equivalent to multiplication in  $\mathbb{Z}/13\mathbb{Z}$ . by prop 2.3. it's commutative.

thus  $Hg_1 = g_1 H$ .

$$\begin{aligned}\alpha = -1, \quad g_1 H &= \{a_1 x^{-1}, \frac{a_1}{3} x^{-1}, \frac{a_1}{9} x^{-1}\} = \{a_1 x^{-1}, \bar{9} a_1 x^{-1}, \bar{3} a_1 x^{-1}\} \\Hg_1 &= \{a_1 x^{-1}, \bar{3} a_1 x^{-1}, \bar{9} a_1 x^{-1}\} = Hg_1. \quad \text{thus } H \triangleleft G.\end{aligned}$$

iii)  $H' = \{\pm x, \pm \bar{3}/x\} = \{x, \bar{3}/x, \bar{10}/x, \bar{12}x\}$

$\bar{2}x \cdot H' = \{\bar{2}x, \bar{9}x, \bar{6}/x, \bar{7}/x\} \quad H' \cdot \bar{2}x = \{\bar{2}x, \bar{9}x, \bar{8}x, \bar{5}x\}$

$\exists g \in G \quad gH' \neq H'g$ .

iv)	$x \cdot H$	$\bar{2}x \cdot H$	$\bar{4}x \cdot H$	$\bar{7}x \cdot H$	$x^{-1} \cdot H$	$\bar{2}x^{-1} \cdot H$	$\bar{4}x^{-1} \cdot H$	$\bar{7}x^{-1} \cdot H$
$x \cdot H$	$x \cdot H$	$\bar{2}x \cdot H$	$\bar{4}x \cdot H$	$\bar{7}x \cdot H$	$x^{-1} \cdot H$	$\bar{2}x^{-1} \cdot H$	$\bar{4}x^{-1} \cdot H$	$\bar{7}x^{-1} \cdot H$
$\bar{2}x \cdot H$	$\bar{2}x \cdot H$	$\bar{4}x \cdot H$	$\bar{7}x \cdot H$	$x \cdot H$	$\bar{2}x^{-1} \cdot H$	$\bar{4}x^{-1} \cdot H$	$\bar{7}x^{-1} \cdot H$	$x^{-1} \cdot H$
$\bar{4}x \cdot H$	$\bar{4}x \cdot H$	$\bar{7}x \cdot H$	$x \cdot H$	$\bar{5}x \cdot H$	$\bar{4}x^{-1} \cdot H$	$\bar{7}x^{-1} \cdot H$	$x^{-1} \cdot H$	$\bar{2}x^{-1} \cdot H$
$\bar{7}x \cdot H$	$\bar{7}x \cdot H$	$x \cdot H$	$\bar{2}x \cdot H$	$\bar{4}x \cdot H$	$\bar{7}x^{-1} \cdot H$	$x^{-1} \cdot H$	$\bar{2}x^{-1} \cdot H$	$\bar{4}x^{-1} \cdot H$
$x^{-1} \cdot H$	$x^{-1} \cdot H$	$\bar{2}x^{-1} \cdot H$	$\bar{4}x^{-1} \cdot H$	$\bar{7}x^{-1} \cdot H$	$x \cdot H$	$\bar{2}x \cdot H$	$\bar{4}x \cdot H$	$\bar{7}x \cdot H$
$\bar{2}x^{-1} \cdot H$	$\bar{2}x^{-1} \cdot H$	$x^{-1} \cdot H$	$\bar{7}x^{-1} \cdot H$	$\bar{4}x^{-1} \cdot H$	$\bar{2}x \cdot H$	$x \cdot H$	$\bar{7}x \cdot H$	$\bar{4}x \cdot H$
$\bar{4}x^{-1} \cdot H$	$\bar{4}x^{-1} \cdot H$	$\bar{2}x^{-1} \cdot H$	$x^{-1} \cdot H$	$\bar{7}x^{-1} \cdot H$	$\bar{4}x \cdot H$	$\bar{2}x \cdot H$	$x \cdot H$	$\bar{7}x \cdot H$
$\bar{7}x^{-1} \cdot H$	$\bar{7}x^{-1} \cdot H$	$\bar{4}x^{-1} \cdot H$	$2x^{-1} \cdot H$	$x^{-1} \cdot H$	$\bar{7}x \cdot H$	$\bar{4}x \cdot H$	$\bar{2}x \cdot H$	$x \cdot H$

Exercise 9.2. Let  $G$  be a group and  $H < G$ . Prove that if  $K(G) \subset H$  then  $H \triangleleft G$ .

Pf:  $\forall g \in G$  and  $h \in H$ .

since  $K(G) \subset H$ . we have  $ghg^{-1} \cdot h^{-1} \in H$ .

by closeness and associativity of subgroup.  $ghg^{-1} = (ghg^{-1}) \cdot (h^{-1} \cdot h) = (ghg^{-1} \cdot h^{-1})h \in H$ .

By lemma 7.3.  $ghg^{-1} \in H$  for all  $g \in G$ ,  $h \in H$  is equivalent to  $H \triangleleft G$ .

Exercise 9.3. Prove that  $K(S_4) = A_4$ .

Pf: i/  $\forall \sigma_1, \sigma_2 \in S_4$ .

by def. of permutation. any permutation and its inverse has same parity.

and in operation of permutation. odd · odd = even even · even = even.

thus we have  $\sigma_1 \sigma_2 \sigma_1^{-1} \sigma_2^{-1} \in A_4$ . thus  $K(S_4) \subset A_4$

ii/ it remains to check  $K(S_4) \supseteq A_4$ .

$A_4 = \{3\text{-cycle}\} \cup \{\text{two disjoint element}\} \cup \{e\}$  denote them be  $B_4$  and  $C_4$  respectively.

we have  $|B_4| = 8$ ,  $|C_4| = 3$ ,  $|K(S_4)| = 1$ .

consider  $B_4$ : 3-cycle means fixed one element. and let them be A, B, C.

we consider only the number in cycle. they have only two forms of permutation. they are  $(CAB)$  and  $(BCA)$ .

$(CAB) = (ACB)(BAC)(ACB)(BAC)$

since  $(ACB)^{-1} = (ACB)$ , and  $(BAC)^{-1} = BAC$ , thus  $(CAB) = (ACB)(BAC)(ACB)^{-1}(BAC)^{-1}$

similarly,  $(BCA) = (BAC)(ACB)(BAC)(ACB) = (BAC)(ACB)(BAC)^{-1}(ACB)^{-1}$

then by inserting. the fixed number into every permutation in above equation,

we can claim that  $B_4 \subset K(S_4)$ .

Consider  $C_4 = \{(2143), (3412), (4321)\}$

$(2143) = (3124)(3241)$ .

where former one is in cycle  $\{\sigma(4) = 4\}$ . latter one in cycle  $\{\sigma(2) = 2\}$ .

$(3412) = (1342)(2314)$ .

where former one is in cycle  $\{\sigma(1) = 1\}$ . latter one in cycle  $\{\sigma(4) = 4\}$ .

$(4321) = (4213)(1423)$ ,

where former one is in cycle  $\{\sigma(2) = 2\}$ . latter one in cycle  $\{\sigma(1) = 1\}$ .

thus.  $C_4 \subset K(S_4)$ , then we have  $A_4 \subset K(S_4)$ . in conclusion  $K(S_4) = A_4$

Exercise 9.4. Find the commutator subgroup of the group  $G$  from Exercise 9.1.

Consider the group  $G = \{ax \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\} \cup \{a/x \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\}$

Sol: we have the formula:

$$\begin{cases} ax \circ a'x = aa'x \\ b/x \circ b'/x = bb'^{-1}x \\ ax \circ b/x = abx^{-1} \\ b/x \circ ax = b/(ax) = b \cdot a^{-1} \cdot x^{-1} \end{cases}$$

denote  $A = \{ax \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\}$   
 $\{a/x \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\}$

thus if  $g \in A$   $g^{-1} = a^{-1}x$ .

if  $g \in B$   $g^{-1} = g$ .

$\forall g_1, g_2 \in G. g_1 g_2 g_1^{-1} g_2^{-1} \in \{ax \mid a \in (\mathbb{Z}/13\mathbb{Z})^*\}$ , i.e.  $K(G) \subseteq A$ .

$\forall g_1 \in A. g_2 \in A. g_1 g_2 g_1^{-1} g_2^{-1} = a_1 \cdot a_2 \cdot a_1^{-1} \cdot a_2^{-1} x$

$a_1 \cdot a_2 \cdot a_1^{-1} \cdot a_2^{-1} = (a_1 \cdot a_1^{-1}) \cdot (a_2 \cdot a_2^{-1}) = \bar{1}$  (by Prop 2.3. multiplication in  $\mathbb{Z}/m\mathbb{Z}$  is commutative)

ii/  $g_1 \in A. g_2 \in B. g_1 g_2 g_1^{-1} g_2^{-1} = (a_1 \cdot a_2) \cdot x^{-1} \circ (a_1^{-1} \cdot a_2) \cdot x^{-1} = (a_1 \cdot a_2)(a_1^{-1} \cdot a_2)^{-1} x$

$(a_1 \cdot a_2)(a_1^{-1} \cdot a_2)^{-1} = a_1 \cdot a_2 \cdot a_2^{-1} \cdot a_1 = a_1 \cdot a_1$ .

iii/  $g_1 \in B. g_2 \in A. g_1 g_2 g_1^{-1} g_2^{-1} = (a_1 \cdot a_2^{-1})x^{-1} \circ (a_1 \cdot a_2) \cdot x^{-1} = (a_1 \cdot a_2^{-1}) \cdot (a_1 \cdot a_2)^{-1} x$

$(a_1 \cdot a_2^{-1}) \cdot (a_1 \cdot a_2)^{-1} = a_1 \cdot a_2^{-1} \cdot a_2^{-1} \cdot a_1^{-1} = a_2^{-1} \cdot a_1^{-1}$

iv/  $g_1 \in B. g_2 \in B. g_1 g_2 g_1^{-1} g_2^{-1} = (a_1 \cdot a_2^{-1})x \circ (a_1 \cdot a_2^{-1})x = a_1 \cdot a_1 \cdot a_2^{-1} \cdot a_2^{-1} x$ .

so the commutator subgroup has the form.  $x$  or  $a \cdot a x$  or  $a_1 \cdot a_1 \cdot a_2 \cdot a_2 x$ .

$$\bar{1} \cdot \bar{1} = \bar{1} \quad \bar{2} \cdot \bar{2} = \bar{4}. \quad \bar{3} \cdot \bar{3} = \bar{9} \quad \bar{4} \cdot \bar{4} = \bar{3} \quad \bar{5} \cdot \bar{5} = \bar{12} \quad \bar{6} \cdot \bar{6} = \bar{10} \quad \underbrace{\bar{7} \cdot \bar{7}}_{=6} = \bar{10} \quad \bar{8} \cdot \bar{8} = \bar{12}$$

$$\bar{3} \cdot \bar{9} = \bar{3} \quad \bar{10} \cdot \bar{10} = \bar{9} \quad \bar{11} \cdot \bar{11} = \bar{4} \quad \bar{12} \cdot \bar{12} = \bar{1} \quad \text{不同再算}.$$

thus the commutator subgroup  $K(G) = \{x, \bar{3}x, \bar{4}x, \bar{9}x, \bar{10}x, \bar{12}x\}$ .

Ex 10.1. Prove that  $\psi: \mathbb{R}^* \rightarrow \mathbb{R}^*$   $\psi(x) = x^2$  is a homomorphism. Find its image and kernel.

Pf:  $\forall x, y \in \mathbb{R}^*. \psi(xy) = (xy)^2 = x^2 y^2 \quad \psi(x)\psi(y) = x^2 y^2$ .

thus  $\psi(xy) = \psi(x)\psi(y)$  for any  $x, y \in \mathbb{R}^*$ .

$$e_{\mathbb{R}^*} = 1. \quad \text{let } \psi(x) = 1 \Rightarrow x^2 = 1 \Rightarrow x = \pm 1 \quad \text{Ker } \psi = \{\pm 1\}.$$

$$\psi(x) = x^2 > 0. \Rightarrow \text{Im } \psi = \{x \mid x \in \mathbb{R} \text{ and } x > 0\}.$$

### Exercise 10.3

Let  $\varphi \in \text{Hom}(G, G')$ .

沒證子群!

i) Prove that  $\varphi^{-1}(H') \triangleleft G$  if  $H' \triangleleft G'$

ii) Prove that  $\varphi(H) \triangleleft \text{Im}(\varphi)$  if  $H \triangleleft G$

i) denote  $\varphi^{-1}(H') = H$ . thus  $\varphi(H) = H'$

$\forall h \in H, \exists h' \in H' \text{ s.t. } \varphi^{-1}(h') = h$ .

$\forall g \in G, \varphi(ghg^{-1}) = \varphi(g) \cdot \varphi(h) \cdot \varphi(g^{-1}) = \varphi(g) \cdot h' \cdot \varphi(g)^{-1}$

by the def. of homomorphism.  $\varphi(g), \varphi(g)^{-1} \in G'$ .

since  $H' \triangleleft G'$ . for all  $h' \in H', g' \in G' \quad g'h'g'^{-1} \in H'$ . (by lemma 7.3).

thus  $\varphi(ghg^{-1}) \in H'$ . i.e.  $ghg^{-1} \in \varphi^{-1}(H')$ ,

which implies  $\varphi^{-1}(H') \triangleleft G$  again by lemma 7.3.

ii).  $\text{Im}(\varphi) \triangleleft G'$  by Prop. 10.3

$\forall h \in H, \forall g \in G$ , we need to check  $\varphi(g) \varphi(h) \varphi(g)^{-1} \in \varphi(H)$ .

since  $H \triangleleft G$ , we have  $ghg^{-1} \in H$ . thus  $\varphi(ghg^{-1}) \in \varphi(H)$

by def. of homomorphism.  $\varphi(g) \varphi(h) \varphi(g)^{-1} = \varphi(g) \varphi(h) \varphi(g^{-1}) = \varphi(ghg^{-1}) \in \varphi(H)$ .

### Exercise 10.4

Find all the endomorphisms of  $\mathbb{Z}/6\mathbb{Z}$ .

Pf:  $\langle \bar{1} \rangle = \mathbb{Z}/6\mathbb{Z}$ . let  $\psi(\bar{1}) = a$ .  $\psi \in \text{End}(\mathbb{Z}/6\mathbb{Z})$ .

by prop 10.5. if  $a$  is defined, the endomorphism is uniquely defined.

①  $\psi(\bar{1}) = \bar{0}$ . trivial endomorphism.  $\psi: x \mapsto \bar{0}$  ⑤  $\psi(\bar{1}) = \bar{4}$

②  $\psi(\bar{1}) = \bar{1}$  identical endomorphism.  $\psi: x \mapsto x$  endomorphism  $\psi:$

③  $\psi(\bar{1}) = \bar{2}$ . endomorphism  $\psi:$

$x$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\psi(x)$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

$x$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\psi(x)$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$

⑥  $\psi(\bar{1}) = \bar{5}$

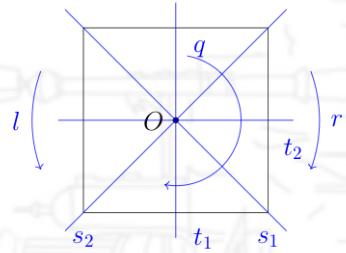
④  $\psi(\bar{1}) = \bar{3}$  endomorphism  $\psi:$

$x$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\psi(x)$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$

$x$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\psi(x)$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Exercise 10.5. Find all the homomorphisms from  $D_4$  to  $\mathbb{Z}/6\mathbb{Z}$ .

	$e$	$r$	$l$	$q$	$t_1$	$t_2$	$s_1$	$s_2$
$e$	$e$	$r$	$l$	$q$	$t_1$	$t_2$	$s_1$	$s_2$
$r$	$r$	$q$	$e$	$l$	$s_2$	$s_1$	$t_1$	$t_2$
$l$	$l$	$e$	$q$	$r$	$s_1$	$s_2$	$t_2$	$t_1$
$q$	$q$	$l$	$r$	$e$	$t_2$	$t_1$	$s_2$	$s_1$
$t_1$	$t_1$	$s_1$	$s_2$	$t_2$	$e$	$q$	$r$	$l$
$t_2$	$t_2$	$s_2$	$s_1$	$t_1$	$q$	$e$	$l$	$r$
$s_1$	$s_1$	$t_2$	$t_1$	$s_2$	$l$	$r$	$e$	$q$
$s_2$	$s_2$	$t_1$	$t_2$	$s_1$	$r$	$l$	$q$	$e$



1) the trivial map always exists.  $\psi(x) = \bar{0}$ .  $x \in D_4$ .

2) find nontrivial homomorphism.

let  $\psi \in \text{Hom}(D_4, \mathbb{Z}/6\mathbb{Z})$ . by lemma 10.1.  $\psi(e) = \bar{0}$

since  $q^2 = e \Rightarrow 2\psi(q) = \bar{0} \Rightarrow \psi(q) = \bar{0}$  or  $\bar{3}$ .

since  $r^2 = q \Rightarrow 2\psi(r) = \psi(q)$ . we can claim that  $\psi(q) \neq \bar{3}$ . otherwise  $\psi(r)$  not exists thus  $\psi(q) = \bar{0}$ .

$$t_1 = t_2 q. \quad s_1 = s_2 q. \quad r = l q. \quad \Rightarrow \quad \psi(s_1) = \psi(s_2) \quad \psi(t_1) = \psi(t_2). \quad \psi(r) = \psi(l)$$

$$s_1 s_2 = q. \quad t_1 t_2 = q. \quad r l = q. \quad \Rightarrow \quad 2\psi(s_1) = 2\psi(t_1) = 2\psi(r) = \bar{0} \rightarrow \text{their} = \bar{3} \text{ or } \bar{0}.$$

i) let  $\psi(s_1) = \bar{3}$ .  $\psi(t_1) = \bar{3}$  then  $\psi(r) = \bar{0}$

ii) let  $\psi(s_1) = \bar{3}$ .  $\psi(t_1) = \bar{0}$  then  $\psi(r) = \bar{3}$

iii) let  $\psi(s_1) = \bar{0}$ .  $\psi(t_1) = \bar{3}$  then  $\psi(r) = \bar{3}$

iv) let  $\psi(s_1) = \bar{0}$ .  $\psi(t_1) = \bar{0}$  then  $\psi(r) = \bar{0}$

- trivial.

In conclusion. 1).  $\begin{array}{c|cccccccc} x & e & r & l & q & t_1 & t_2 & s_1 & s_2 \\ \hline \psi(x) & \bar{0} \end{array}$

homomorphism define as: 2)  $\begin{array}{c|cccccccc} x & e & r & l & q & t_1 & t_2 & s_1 & s_2 \\ \hline \psi(x) & \bar{0} & \bar{0} & \bar{0} & \bar{0} & \bar{3} & \bar{3} & \bar{3} & \bar{3} \end{array}$

3)  $\begin{array}{c|cccccccc} x & e & r & l & q & t_1 & t_2 & s_1 & s_2 \\ \hline \psi(x) & \bar{0} & \bar{3} & \bar{3} & \bar{0} & \bar{3} & \bar{3} & \bar{0} & \bar{0} \end{array}$

4)  $\begin{array}{c|cccccccc} x & e & r & l & q & t_1 & t_2 & s_1 & s_2 \\ \hline \psi(x) & \bar{0} & \bar{3} & \bar{3} & \bar{0} & \bar{0} & \bar{0} & \bar{3} & \bar{3} \end{array}$

Exercise 11.1. Let  $G, H$  be isomorphic groups and  $G$  can be generated by two elements. Show that  $H$  satisfies the same property.

Pf: let  $G = \langle a, b \rangle$ .

$\forall g \in G. \quad g = a^{Nq_1} b^{Nq_2}, \quad Nq_1, Nq_2 \in \mathbb{Z}$ .

$\psi$  is a bijection.  $\forall h \in H. \exists! g. \quad \psi(g) = h$ .

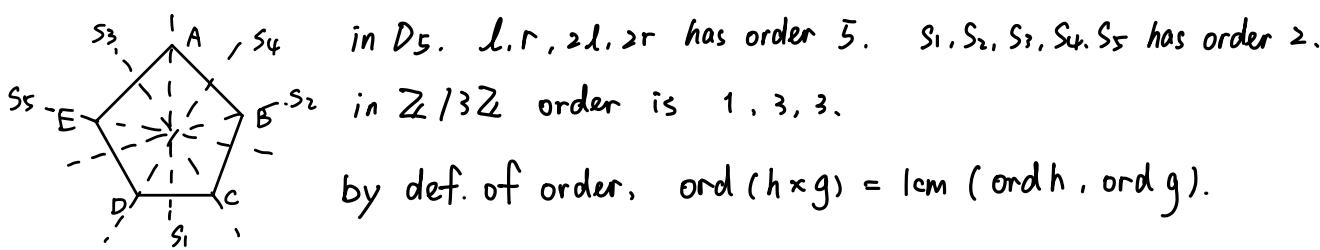
i.e.  $h = \psi(a^{Nq_1} b^{Nq_2}) = \psi(a^{Nq_1}) * \psi(b^{Nq_2}) = \psi(a)^{Nq_1} * \psi(b)^{Nq_2}$ .

Since  $h$  is arbitrary.  $H = \langle \psi(a), \psi(b) \rangle$

Exercise 11.2. Prove that  $D_3 \times \mathbb{Z}/5\mathbb{Z} \not\cong D_5 \times \mathbb{Z}/3\mathbb{Z}$

Pf: in  $D_3$ , l.r has order 3.  $S_1, S_2, S_3$  order 2.

in  $\mathbb{Z}/5\mathbb{Z}$ , order is 1, 5, 5, 5, 5



in  $D_3 \times \mathbb{Z}/5\mathbb{Z}$   $S_1 \times 1$  has order 10.

where in  $D_5 \times \mathbb{Z}/3\mathbb{Z}$ , the possible order is 1, 2, 3, 5, 6, 15. No order 10.

by Prop 11.3 it doesn't satisfy the necessary condition of existence of isomorphisms.

Exercise 11.3. Prove that  $\mathbb{Q} \not\cong \mathbb{Q} \times \mathbb{Q}$

Hint. For any  $p, q \in \mathbb{Q}$ , there is  $r \in \mathbb{Q}$  such that both  $p$  and  $q$  are multiples of  $r$ .

Pf:  $\forall \frac{p}{q} \in \mathbb{Q}, p, q \in \mathbb{Z} \setminus \{0\}$ .  $\text{gcd}(p, q) = 1$ . denote  $r = \text{lcm}(p, q)$ .

Assume the converse.  $\exists \psi$  isomorphism and set  $\psi(1) = (a, b)$   $a, b$  arbitrary in  $\mathbb{Q}$

then, for any  $n \in \mathbb{Z} \setminus \{0\}$   $\psi(n) = \psi(n \cdot \frac{1}{n}) = n \psi(\frac{1}{n}) = (a, b) \Rightarrow \psi(\frac{1}{n}) = \frac{1}{n} (a, b)$ .

$$\psi(\frac{p}{q}) = p \cdot \psi(\frac{1}{q}) = \frac{p}{q} (a, b) \text{ for any } \frac{p}{q} \in \mathbb{Q}.$$

now consider  $(a, b+1)$  assume  $\exists \frac{p_1}{q_1} \in \mathbb{Q}$  s.t.  $\psi(\frac{p_1}{q_1}) = (a, b+1)$ .

i.e.  $(a, b+1) = \frac{p_1}{q_1} (a, b) \Rightarrow \begin{cases} a = \frac{p_1}{q_1} a \\ b+1 = \frac{p_1}{q_1} b \end{cases}$  no solution, which means  $\psi$  is not bijective.

since  $(a, b)$  and  $\frac{p}{q}$  are arbitrary, no bijection  $\psi$  can be isomorphism between  $\mathbb{Q}$  and  $\mathbb{Q} \times \mathbb{Q}$ .

thus  $\mathbb{Q} \not\cong \mathbb{Q} \times \mathbb{Q}$

Exercise 11.4. For  $G = \text{GL}_n(\mathbb{C})$ ,  $H = \{A \in \text{GL}_n(\mathbb{C}) \mid \det A = \pm 1, \pm i\}$ , show that  $G/H \cong \mathbb{C}^*$

Pf: by thm 11.5. it suffices to find  $\psi \in \text{Hom}(G, H)$ . s.t.  $\text{Ker}(\psi) = H$  and  $\text{Im}(\psi) = \mathbb{C}^*$

$$\text{let } \psi(A) = \left( \frac{\det A}{|\det A|} \right)^4 \cdot |\det A|$$

since  $(i)^4 = (-i)^4 = (1)^4 = (-1)^4 = 1 = e_{\mathbb{C}^*}$ .  $\text{Ker } \psi = H$ .

$$\text{Im} \left( \frac{\det A}{|\det A|} \right)^4 = T, \text{ Im } |\det A| \in \mathbb{R}_+, \text{ thus } \text{Im } (\psi) = \mathbb{C}^*$$

$$\begin{aligned} \forall A, B \in G. \psi(AB) &= \left( \frac{\det AB}{|\det AB|} \right)^4 \cdot |\det AB| = \left( \frac{\det A}{|\det A|} \right)^4 \cdot \left( \frac{\det B}{|\det B|} \right)^4 \cdot |\det A| \cdot |\det B| \\ &= \left[ \left( \frac{\det A}{|\det A|} \right)^4 |\det A| \right] \cdot \left[ \left( \frac{\det B}{|\det B|} \right)^4 |\det B| \right] = \psi(A) \cdot \psi(B), \text{ i.e. } \psi \in \text{Hom}(G, H) \end{aligned}$$

In conclusion,  $G/H \cong \mathbb{C}^*$

$$\text{in } \mathbb{Q}. \forall g_1, g_2 \in G. \exists g \in G. g_1 \circ g^n \circ g_2 = g^m. m, n \in \mathbb{Z}$$

$$g_1 = \frac{m_1}{n_1}, g_2 = \frac{m_2}{n_2}, g = \frac{1}{m_1 n_2}$$

Assume.  $\psi: G \rightarrow G'$  - isomorphic.

$$\forall \varphi(g), \psi(g) \in G'. \exists g, g = g^n \circ g^m. \Rightarrow \psi(g) = \psi(g^n) = \psi(g)^n$$

$$\psi(g) = \psi(g^m) = \psi(g)^m.$$

i.e.  $\exists \psi(g). \psi(g) = \psi(g)^n, \psi(g) = \psi(g)^m$ .

$$\text{let } (1, 0), (0, 1) \in \mathbb{Q} \times \mathbb{Q}. \exists (r, s) \in \mathbb{Q} \times \mathbb{Q}$$

$$(1, 0) = r(1, 0)$$

$$(0, 1) = s(1, 0)$$

isomorphism preserve this property

# HW4. Week 13th.

**Exercise 12.1.** Prove that any abelian group of order 8 is isomorphic to one of the following groups:  $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

*Hint.* Show that  $G = \{0, a, b, c, a+b, a+c, b+c, a+b+c\}$  if there are distinct  $a, b, c \in G$  of order 2 with  $c \neq a+b$ . Show that  $G = \{0, a, 2a, 3a, b, a+b, 2a+b, 3a+b\}$  if  $\text{ord } a = 4$  and  $b \neq 0, a, 2a, 3a$ .

**Pf:** Let  $|G| = 8$ . by Coro 8.4. the order of non-identity element can be 2, 4 or 8.

i) if  $\exists a$ ,  $\text{ord } a = 8$ . then  $\langle a \rangle = G$ .  $G$  is cyclic group. thus  $G \cong \mathbb{Z}/8\mathbb{Z}$ . by thm 12.1.

ii) if  $\text{ord } a_i = 2$  for  $i=1, \dots, 7$ . in this case we need at least 3 elements except e.

otherwise, if we only have 2 non-identity elements in generator set,  $G = \{e, a_1, a_2, a_1 a_2\}$ .  $|G|=4$ .

$G \cong \{e_1, a_1\} \times \{e_2, a_2\} \times \{e_3, a_3\}$ . s.t.  $a_1 + a_2 \neq a_3$ .

thus.  $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . the isomorphism maps.  $e_i \mapsto \bar{0}$   $a_i \mapsto \bar{i}$  (in  $i$ th place)

iii) if there exists  $\text{ord } a = 4$ , denote  $H = \{e, a, a^2, a^3\}$

by Lagrange thm.  $|G:H| = \frac{|G|}{|H|} = 2$ . since  $eH$  always exists. then the non-identity left coset of  $H$  is unique. denote by  $bH$ , thus  $G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$

by the cancellation law of group and  $a \neq b \neq e$ . the elements are distinct.  $|G|=8$ .

define a map  $\psi: G \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .  $\psi(e) = (\bar{0}, \bar{0})$   $\psi(a) = (\bar{1}, \bar{0})$   $\psi(b) = (\bar{0}, \bar{1})$ .

check the 8 elements one by one. using above laws of mapping.  $\psi \in \text{Hom}(G, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$

and  $\psi$  is bijective. thus.  $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

The discussion of orders of elements in  $G$ . ensures that no other cases.

**Exercise 12.2.** Let  $p$  be a prime,  $G$  be a finite abelian group and  $\text{ord } g = p$  for any non-zero  $g \in G$ . Prove that  $G$  is isomorphic to  $\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$ .

*Hint.*  $G$  can be considered as a vector space over  $\mathbb{Z}/p\mathbb{Z}$ .

**Pf:** Consider  $G$  as a vector space over  $\mathbb{Z}/p\mathbb{Z}$ :

addition is the operation of group. scalar multiplication :  $a \cdot g = g^a$   $a \in \mathbb{Z}/p\mathbb{Z}$ ,  $g \in G$ .

check axioms: associativity of addition, existence of identity elements, existence of additive inverse.

commutative of addition. satisfy by def. of abelian group.

$\forall a, b \in \mathbb{Z}/p\mathbb{Z}$ .  $g_1, g_2 \in G$ .  $\bar{1} \cdot g = g^{\bar{1}} = g$ .

$$a(g_1 * g_2) = (g_1 * g_2)^a = g_1^a * g_2^a \quad (a+b)g_1 = g_1^{a+b} = g_1^a * g_1^b = ag_1 + bg_1 \quad \text{by prop 6.1.}$$

$$a \cdot (b \cdot g_1) = a(g_1^b) = (g_1)^{ba} = (g_1)^{ab} = (a \cdot b) \cdot g_1 \quad \text{by prop 6.1. and commutativity in } \mathbb{Z}/p\mathbb{Z}.$$

$G$  is finite. it's dimension is finite as well. let  $\dim G = n$ . thus.  $|G| = p^n$

now we define the basis.  $\{g_i\}_{i \in [1:n]}$ .

$$\forall g \in G, \exists \{\varepsilon_1, \dots, \varepsilon_n\} \quad \varepsilon_i \in \mathbb{Z}/p\mathbb{Z} \quad \text{s.t. } g = \sum \varepsilon_i g_i \quad \text{i.e. } g = g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_n^{\varepsilon_n}$$

For  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$ . we have the basis.  $\{e_i\}_{i \in [1:n]} \quad e_i = (\bar{0}, \dots, \bar{i}, \dots, \bar{0})$   $\bar{i}$  appears in  $i$ th place.

$$\forall a = (a_1, \dots, a_n) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}. \text{ we have } a_i \in \mathbb{Z}/p\mathbb{Z} \text{ and } a = \sum_{i=1}^n a_i e_i$$

by corresponding.  $\{\varepsilon_1, \dots, \varepsilon_n\}$  to  $\{a_1, \dots, a_n\}$ . we construct the bijection. (1-to-1 corr.)

$$\psi: \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z} \rightarrow G \quad \text{s.t. } \psi(a) = \psi(\sum a_i e_i) = \sum a_i \psi(e_i) = \sum a_i g_i = g$$

And since  $\psi(a) \psi(b) = \psi(\sum a_i e_i) \psi(\sum b_i e_i) = \sum (a_i b_i) \psi(e_i) = \psi(ab)$ .

$\psi \in \text{Hom}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}, G)$ . whence  $\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z} \cong G$ .

**Exercise 13.1.** Let a group  $G$  act on a set  $M$ . Prove that  $G_m \cong G_{m'}$  if  $m, m'$  belong to the same orbit.

Hint.  $G_m$  and  $G_{m'}$  are conjugates, that is  $G_{m'} = g G_m g^{-1}$  for some  $g \in G$ .

Pf:  $m, m'$  belongs to the same orbit. i.e.  $\exists g_0 \in G$  s.t.  $m' = g_0 m \quad \exists g_1 \in G$  s.t.  $m = g_1 m'$

$\forall h \in G_m$ . consider conjugation  $h' = g_0 h g_0^{-1}$

$$h' m' = g_0 h g_0^{-1} m' = g_0 h g_0^{-1} \cdot g_0 \cdot m = g_0(hm) = g_0 m = m'. \text{ thus } h' \in G_{m'}$$

$\forall h' \in G_{m'}$  consider conjugation  $h = g_1 h' g_1^{-1}$

$$hm = g_1 h' g_1^{-1} m = g_1 h' g_1^{-1} \cdot g_1 m' = g_1 h' m' = g_1 m' = m \text{ thus } h \in G_m.$$

Thus  $G_m$  and  $G_{m'}$  are conjugates

denote map  $\psi: G_m \rightarrow G_{m'} \quad \psi(h) = g_0 h g_0^{-1}$

$$\forall h_1, h_2 \in G_m \quad \psi(h_1) \psi(h_2) = g_0 h_1 (g_0^{-1} \cdot g_0) h_2 g_0^{-1} = g_0(h_1 h_2) g_0^{-1} = \psi(h_1 h_2). \text{ (by associativity)}$$

thus  $\psi \in \text{Hom}(G_m, G_{m'})$ .

since the conjugation.  $\text{Im } \psi = G_{m'}$ . Surjective.

let  $\psi(h_1) = \psi(h_2)$ ,  $g_0 h_1 g_0^{-1} = g_0 h_2 g_0^{-1}$ . by cancellation law in subgroup  $G_{m'}$ ,  $h_1 = h_2$ .

thus  $\psi$  is bijective. whence it's isomorphism, i.e.  $G_m \cong G_{m'}$

**Exercise 13.2.** Let  $G = \{A \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \mid AA^T = E_2\}$ . Find the orbits and the stabilizers for its action on  $\mathrm{M}_{2,1}(\mathbb{Z}/3\mathbb{Z})$  by multiplication.

Hint.

$$G = \left\{ \begin{pmatrix} \bar{1}, \bar{0} \\ \bar{0}, \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1}, \bar{0} \\ \bar{0}, \bar{2} \end{pmatrix}, \begin{pmatrix} \bar{0}, \bar{1} \\ \bar{1}, \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0}, \bar{1} \\ \bar{2}, \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0}, \bar{2} \\ \bar{1}, \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0}, \bar{2} \\ \bar{2}, \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{2}, \bar{0} \\ \bar{0}, \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{2}, \bar{0} \\ \bar{0}, \bar{2} \end{pmatrix} \right\}$$

Solution:  $|M| = 9$

$$1) \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \begin{pmatrix} \bar{0} \\ \bar{b} \end{pmatrix} = \begin{pmatrix} \bar{b} \\ \bar{a} \end{pmatrix} \quad (\bar{1} \bar{0}) (\bar{0} \bar{2}) = (\bar{0} \bar{2})$$

$(\bar{1} \bar{0}), (\bar{0} \bar{1}), (\bar{2} \bar{0}), (\bar{0} \bar{2})$  in same orbit it's corresponding  $|G_{m_1}| = \frac{|G|}{|\mathrm{Orb}_{m_1}|} = 2$ .

$$\mathrm{Orb}_{m_1} = \left\{ \begin{pmatrix} \bar{1} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} \\ \bar{2} \end{pmatrix} \right\}$$

$$G_{(\bar{1} \bar{0})} = G_{(\bar{0} \bar{1})} = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix} \right\}. \quad G_{(\bar{0} \bar{2})} = G_{(\bar{2} \bar{0})} = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{2} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \right\}.$$

2)  $g m_2 = m_2 = \begin{pmatrix} \bar{0} \\ \bar{0} \end{pmatrix}$  for any  $g \in G$ . it's corresponding  $G_{m_2} = G$ .

$$\mathrm{Orb}_{m_2} = \left\{ \begin{pmatrix} \bar{0} \\ \bar{0} \end{pmatrix} \right\} \quad G_{m_2} = G.$$

3)  $(\bar{2} \bar{0}) (\bar{0} \bar{2}) (\bar{1} \bar{1}) = (\bar{2} \bar{0}), (\bar{2} \bar{0}) (\bar{1} \bar{1}) = (\bar{2} \bar{1}), (\bar{0} \bar{1}) (\bar{1} \bar{1}) = (\bar{1} \bar{2})$   $|\mathrm{Orb}_{m_3}| = 4$ , it's corresponding  $|G_{m_3}| = \frac{|G|}{|\mathrm{Orb}_{m_3}|} = 2$

$$\mathrm{Orb}_{m_3} = \left\{ \begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{2} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{2} \end{pmatrix} \right\}.$$

$$G_{(\bar{1} \bar{1})} = G_{(\bar{2} \bar{1})} = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \right\} \quad G_{(\bar{1} \bar{2})} = G_{(\bar{2} \bar{2})} = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{2} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{2} & \bar{0} \end{pmatrix} \right\}$$

**Exercise 13.3.** Find the number of rotationally distinct colorings of the faces of a cube using three colors.

Hint. The group of the rotational symmetries of a cube consists of the following 24 elements: the identity, the rotations through  $120^\circ$  and  $240^\circ$  about 4 axes connecting the opposite vertices of the cube, the rotations through  $180^\circ$  about 6 axes connecting the midpoints of the opposite edges, and the rotations through  $90^\circ$ ,  $180^\circ$  and  $270^\circ$  about 3 axes connecting the centers of the opposite faces.

考虑 cycle 是因为在 cycle 上颜色必须是一致的，否则不可能有“最后不变”。

For each type of rotations, define some number to describe the face

$$1) \begin{array}{ccccccc} \text{cube} & \begin{array}{c} \text{1} \\ \text{2} \\ \text{3} \\ \text{4} \\ \text{5} \\ \text{6} \end{array} & 120^\circ & \text{2 cycle} & \begin{array}{c} 1 \xrightarrow{5} \\ \nwarrow 4 \downarrow \\ 5 \xleftarrow{4} \\ \uparrow 6 \end{array} & \begin{array}{c} 2 \xleftarrow{3} \\ \uparrow 6 \downarrow \\ 3 \xleftarrow{6} \\ \uparrow 2 \end{array} & |M^9| = 3^2 \quad 4 \text{ axes} \\ & \begin{array}{c} \text{1} \\ \text{2} \\ \text{3} \\ \text{4} \\ \text{5} \\ \text{6} \end{array} & 240^\circ & \text{2 cycle} & \begin{array}{c} 1 \leftarrow 5 \\ \uparrow 4 \downarrow \\ 5 \leftarrow 4 \\ \uparrow 6 \end{array} & \begin{array}{c} 2 \leftarrow 3 \\ \uparrow 6 \downarrow \\ 3 \leftarrow 6 \\ \uparrow 2 \end{array} & |M^9| = 3^2 \quad 4 \text{ axes} \end{array}$$

$$2) \begin{array}{ccccccc} \text{cube} & \begin{array}{c} \text{1} \\ \text{2} \\ \text{3} \\ \text{4} \\ \text{5} \\ \text{6} \end{array} & 180^\circ & \text{3 cycle} & \begin{array}{c} 1 \rightleftharpoons b \\ 2 \rightleftharpoons 3 \\ 4 \rightleftharpoons 5 \end{array} & \begin{array}{c} 1 \rightleftharpoons b \\ 2 \rightleftharpoons 3 \\ 4 \rightleftharpoons 5 \end{array} & |M^9| = 3^3 \quad 6 \text{ axes} \\ & \begin{array}{c} \text{1} \\ \text{2} \\ \text{3} \\ \text{4} \\ \text{5} \\ \text{6} \end{array} & & & & & \end{array}$$

$$3) \begin{array}{ccccccc} \text{cube} & \begin{array}{c} \text{1} \\ \text{2} \\ \text{3} \\ \text{4} \\ \text{5} \\ \text{6} \end{array} & 90^\circ, 270^\circ & \text{3 cycle} & \begin{array}{c} (1), (6) \\ (1), (6) \end{array} & \begin{array}{c} 90^\circ \quad 5 \xrightarrow[270^\circ]{\nwarrow} 3 \\ \uparrow \quad \uparrow \\ 270^\circ \quad 5 \xrightarrow[270^\circ]{\nwarrow} 3 \end{array} & |M^9| = 3^3 \times 2. \quad 3 \text{ axes} \\ & \begin{array}{c} \text{1} \\ \text{2} \\ \text{3} \\ \text{4} \\ \text{5} \\ \text{6} \end{array} & 180^\circ & \text{4 cycle} & \begin{array}{c} (1), (6) \\ (1), (6) \end{array} & \begin{array}{c} 2 \rightleftharpoons 4 \\ 3 \rightleftharpoons 5 \end{array} & |M^9| = 3^4 \quad 3 \text{ axes} \end{array}$$

$$\sum |M^9| = 3^2 \times 4 + 3^2 \times 4 + 3^3 \times 6 + 3^3 \times 2 \times 3 + 3^4 \times 3 + 3^6 = 1368$$

$$\text{by Burnside lemma. } N = \frac{\sum |M^9|}{|G|} = 57$$

## HW5. Week 14 th.

**Exercise 15.1.** Let  $R$  be a ring. Prove that  $a^2 + (-b^2) = (a+b)(a+(-b))$  for any  $a, b \in R$ . Refer to each axiom or property you use.

$$\begin{aligned}
 \text{Pf: } a^2 + (-b^2) &= a^2 + (-b^2) + a \cdot b - b \cdot a \quad (\text{commutativity of } \cdot) \\
 &= (a^2 + a \cdot b) + [(-b) \cdot b + (-b) \cdot a] \quad (\text{commutativity, associativity of } +; \text{ lemma 15.1.2.}) \\
 &= a(a+b) + (-b)(b+a) \quad (\text{left distributivity}) \\
 &= [a + (-b)](a+b) \quad (\text{commutativity of } +, \text{ right distributivity}) \\
 &= (a+b)(a+(-b)) \quad (\text{commutativity of } \cdot)
 \end{aligned}$$

**Exercise 15.2.** Prove that every finite integral domain is a field

*Hint.* Show that if  $x \neq 0$  then  $x^n = 1$  for a certain  $n \in \mathbb{N}$ .

Pf: denote an arbitrary integral domain by  $R$ .

We claim that  $\forall x \in R, x \neq 0, x^n = 1$  for some  $n \in \mathbb{N}$ . Assume the converse.  $\exists x \in R, \text{char}(x) = 0$  by the def. of ring, we have  $x^i \in R$  for any  $i \in \mathbb{N}$ .

and we claim that  $x^i \neq x^j$  for any  $i \neq j$ , otherwise  $x^{j-i} = 1$  by Prop. 15.2.

thus. distinct  $x, x^2, x^3, \dots, x^n, \dots \in R$ . contradicts with the finiteness of  $R$ .

Whence,  $\forall x \in R, x \neq 0, \exists x^{n-1} = x^{-1}$ , s.t.  $x^{n-1} \cdot x = x \cdot x^{n-1} = 1$ . thus  $R$  is a field.

**Exercise 15.3.** Let  $F = \{(a, b) \mid a, b \in \mathbb{Z}/3\mathbb{Z}\}$ . Define on  $F$  two operations:

$$(a, b) + (c, d) = (a+c, b+d), \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Show that  $F$  with respect to the above operations is a field of characteristic 3 proving explicitly

- Distributivity of multiplication over addition
- Existence of multiplicative inverses
- $\text{char } F = 3$

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}.$$

*Hint.* Notice that  $(\bar{0}, \bar{1})^2 = (-\bar{1}, \bar{0})$ . One can associate  $(a, b)$  with  $a+bi$  where  $i^2 = -1$ .

Pf: (1).  $\forall (a_1, b_1), (a_2, b_2), (a_3, b_3) \in F$ .

$$\text{LHS} = (a_1, b_1) \cdot [(a_2, b_2) + (a_3, b_3)] = (a_1, b_1) \cdot (a_2 + a_3, b_2 + b_3) = a_1(a_2 + a_3) - b_1(b_2 + b_3), \quad a_1(b_2 + b_3) + b_1(a_2 + a_3)$$

$$\text{RHS} = (a_1, b_1) \cdot (a_2, b_2) + (a_1, b_1) \cdot (a_3, b_3) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1) + (a_1 a_3 - b_1 b_3, a_1 b_3 + b_1 a_3).$$

$$= (a_1 a_2 + a_1 a_3 - b_1 b_2 - b_1 b_3, a_1 b_2 + a_1 b_3 + b_1 a_2 + b_1 a_3) = \text{LHS}.$$

$$\text{LHS} = [(a_1, b_1) + (a_2, b_2)] \cdot (a_3, b_3) = (a_1 + a_2, b_1 + b_2) \cdot (a_3, b_3) = ((a_1 + a_2)a_3 - (b_1 + b_2)b_3, (a_1 + a_2)b_3 + (b_1 + b_2)a_3)$$

$$\text{RHS} = (a_1, b_1) \cdot (a_3, b_3) + (a_2, b_2) \cdot (a_3, b_3) = (a_1 a_3 - b_1 b_3, a_1 b_3 + b_1 a_3) + (a_2 a_3 - b_2 b_3, a_2 b_3 + a_3 b_2)$$

$$= (a_1 a_3 + a_2 a_3 - b_1 b_3 - b_2 b_3, a_1 b_3 + a_2 b_3 + b_1 a_3 + b_2 a_3) = \text{LHS}.$$

$$(2). \forall (a, b) \in F^*. \exists \left( \frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \right), \text{ since } \mathbb{Z}/3\mathbb{Z} \text{ is a field, } \frac{1}{a^2+b^2} \in \mathbb{Z}/3\mathbb{Z}, \text{ and } \frac{a}{a^2+b^2} \in \mathbb{Z}/3\mathbb{Z}.$$

$$\text{thus } \left( \frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \right) \in F \text{ and } (a, b) \cdot \left( \frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \right) = (\bar{1}, \bar{0}).$$

$$(3) (\bar{1}, \bar{0})\text{-unity of } F \quad (\bar{1}, \bar{0}) + (\bar{1}, \bar{0}) = (\bar{2}, \bar{0}) \neq \bar{0}. \quad (\bar{1}, \bar{0}) + (\bar{1}, \bar{0}) + (\bar{1}, \bar{0}) = (\bar{0}, \bar{0}) = \bar{0}$$

Exercise 15.4. Let

$$F = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

- i) Show that  $F$  is a ring with respect to matrix addition and multiplication.
- ii) Show that  $F$  is isomorphic to  $\mathbb{C}$  by considering  $\Phi: F \rightarrow \mathbb{C}$ ,

$$\Phi \left( \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right) = a + bi.$$

i). I. associative of  $+$  by the associativity of every entry (associativity of " $+$ " over  $\mathbb{R}$ )

$$\text{II. } \exists \vec{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ s.t. } \forall A \in F. A + \vec{0} = \vec{0} + A = A.$$

$$\text{III. } \forall A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}. \exists A' = \begin{pmatrix} -a & -b \\ b & -a \end{pmatrix} \quad A + A' = A' + A = \vec{0}$$

IV commutative of  $+$  by the commutativity of every entry (commutativity of " $+$ " over  $\mathbb{R}$ )

V. distributivity is shown by distributivity of matrix operation.

$$A(B+C) = AB+AC \quad (A+B)C = AC+BC \text{ for any matrix.}$$

VI. similar as V.  $A \cdot (B \cdot C) = (A \cdot B) \cdot C$  for any matrix.

$$\text{VII. } \exists E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \text{ s.t. } \forall A \in F. \text{ s.t. } AE = EA = A.$$

$$\text{VIII. } \forall \begin{pmatrix} a_i & b_i \\ -b_i & a_i \end{pmatrix} \in F. i=1,2 \quad \text{LHS} = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -a_2b_1 - a_1b_2 & -b_1b_2 + a_1a_2 \end{pmatrix}$$

$$\text{RHS} = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_2b_1 + a_1b_2 \\ -a_1b_2 - b_1a_2 & -b_1b_2 + a_1a_2 \end{pmatrix} = \text{LHS.}$$

ii)  $\forall A_1, A_2 \in F$ .

$$\Phi(A_1 + A_2) = \Phi \left( \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ -b_1 - b_2 & a_1 + a_2 \end{pmatrix} \right) = (a_1 + a_2) + (b_1 + b_2)i = (a_1 + b_1i) + (a_2 + b_2i) = \Phi(A_1) + \Phi(A_2).$$

$$\Phi(A_1 A_2) = \Phi \left( \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -a_2b_1 - a_1b_2 & -b_1b_2 + a_1a_2 \end{pmatrix} \right) = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i = (a_1 + b_1i)(a_2 + b_2i) = \Phi(A_1) \cdot \Phi(A_2)$$

Exercise 15.5. Show that  $\mathbb{Z}[\sqrt{2}]$  and  $\mathbb{Z}[\sqrt{3}]$  are not isomorphic.

Hint. If an isomorphism exists, consider the image of  $\sqrt{2}$  under it.

Pf: Assume the converse.  $\exists \Phi: \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}[\sqrt{3}]$

consider  $\Phi(\sqrt{2}) = a + b\sqrt{3}$ ,  $a, b \in \mathbb{Z}$ .

$$\Phi(2) = \Phi(\sqrt{2}) \cdot \Phi(\sqrt{2}) = a^2 + 3b^2 + 2ab\sqrt{3}$$

but. we have  $\Phi(e_{\mathbb{Z}[\sqrt{2}]}) = e_{\mathbb{Z}[\sqrt{3}]}$  where  $e$  is the unity.

(by cancellation law).

$$\text{since } e_{\mathbb{Z}[\sqrt{2}]} \cdot e_{\mathbb{Z}[\sqrt{2}]} = e_{\mathbb{Z}[\sqrt{2}]} \Rightarrow \Phi(e_{\mathbb{Z}[\sqrt{2}]}) \cdot \Phi(e_{\mathbb{Z}[\sqrt{2}]}) = \Phi(e_{\mathbb{Z}[\sqrt{2}]}) \Rightarrow \Phi(e_{\mathbb{Z}[\sqrt{2}]}) = e_{\mathbb{Z}[\sqrt{3}]}.$$

$$e_{\mathbb{Z}[\sqrt{2}]} = e_{\mathbb{Z}[\sqrt{3}]} = 1 \quad \text{thus.} \quad \Phi(2) = \Phi(1) + \Phi(1) = 1 + 1 = 2. \quad \text{contradicts.}$$

Exercise 16.1. Let  $I, J$  be ideals of  $R$ . Define

$$I + J = \{a + b \mid a \in I, b \in J\}, \quad IJ = \{a_1 b_1 + \cdots + a_n b_n \mid a_1, \dots, a_n \in I, b_1, \dots, b_n \in J\}.$$

i) Prove that  $I + J, IJ$  are ideals of  $R$

ii) Prove that  $I(J + J') = IJ + IJ'$

iii) Find a generating set for  $IJ$  if  $I = (a_1, \dots, a_n), J = (b_1, \dots, b_m)$

Pf: i).  $I + J \quad \forall a_i + b_1, a_2 + b_2 \in I + J, r \in R.$

$$\textcircled{1} (a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2) \in I + J, \text{ since } I, J \text{ are ideal. } a_1 + a_2 \in I. b_1 + b_2 \in J.$$

$$\textcircled{2} r(a_1 + b_1) = ra_1 + rb_1. \text{ (by distributivity of Ring.) since } I, J \text{ are ideal. } ra_1 \in I. rb_1 \in J.$$

$$\text{ii) } IJ \quad \forall \sum_{i=1}^{N_1} a_i^1 b_i^1, \sum_{j=1}^{N_2} a_j^2 b_j^2 \in IJ. r \in R.$$

$$\textcircled{1} \text{ denote } N = \max(N_1, N_2) \text{ since } 0 \in I. \text{ denote } a_j^2. a_i^1 = 0 \text{ where } N_1+1 \leq i \leq N, N_2+1 \leq j \leq N.$$

$$\sum_{i=1}^{N_1} a_i^1 b_i^1 + \sum_{j=1}^{N_2} a_j^2 b_j^2 = \sum_{i=1}^{N_1+N_2} a_i^1 b_i^1 \text{ (by rearranging them). } \in IJ.$$

$$\textcircled{2} r \sum_{i=1}^{N_1} a_i^1 b_i^1 = \sum_{i=1}^{N_1} (ra_i^1) b_i^1 \in IJ. \text{ since } I \text{ is an ideal. so } ra_i^1 \in I. \text{ and } b_i^1 \in J$$

$$\text{ii) } \forall \sum_{i=1}^{N_1} a_i^1 b_i^1 \in J \quad \sum_{j=1}^{N_2} a_j^2 b_j^2 \in J' \quad a \in I.$$

$$\text{for } a \left( \sum_{i=1}^{N_1} a_i^1 b_i^1 + \sum_{j=1}^{N_2} a_j^2 b_j^2 \right) = a \sum_{i=1}^{N_1} a_i^1 b_i^1 + a \sum_{j=1}^{N_2} a_j^2 b_j^2 = \sum_{i=1}^{N_1} (aa_i^1) b_i^1 + \sum_{j=1}^{N_2} (aa_j^2) b_j^2$$

$$a \in I, a_i^1, a_j^2 \in I \quad I \text{ is ideal. } \Rightarrow (aa_i^1) \in I, (aa_j^2) \in I, \text{ thus } \sum_{i=1}^{N_1} (aa_i^1) b_i^1 + \sum_{j=1}^{N_2} (aa_j^2) b_j^2 \in I(J + J').$$

$$\text{thus we have } I(J + J') \subseteq IJ + IJ'$$

similarly we can check  $I(J + J') \supseteq IJ + IJ'$  by distributivity of  $R$ .

$$\text{iii) } I = (a_1, \dots, a_n) = \left\{ r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_i \in R, i \in [1:n] \right\}$$

$$J = (b_1, \dots, b_m) = \left\{ p_1 b_1 + p_2 b_2 + \cdots + p_m b_m \mid p_j \in R, j \in [1:m] \right\}.$$

$$IJ = \left\{ \sum_k \left( \sum_{i=1}^{n_k} r_i a_i \right) \left( \sum_{j=1}^{m_k} p_j b_j \right) = \sum_k \left( \sum_{i,j} r_i p_j a_i b_j \right) \right\}$$

$$k \text{ can be arbitrary in } \mathbb{Z}_+. \quad r_i \in R, p_j \in R. \Rightarrow r_i p_j \in R.$$

$$\text{thus } IJ = (a_i b_j \mid i \in [1:n], j \in [1:m]).$$

Exercise 16.2. Let  $\xi$  be a complex cube root of 1. For  $R = \mathbb{Z}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Z}\}$ , find  $R^*$ .

Hint. Define  $N$  similarly to Problem 16.5.

$$\text{Pf. } \xi^3 = 1. \quad \begin{array}{c} \nearrow \\ \xi = e^{\frac{2\pi i k}{3}} \end{array} \quad \begin{array}{c} \searrow \\ 1/\xi = 1 \quad a+b \in \mathbb{Z}. \end{array}$$

$$\text{if } \xi \neq 1. \quad |a+b\xi| = \sqrt{(a+b\xi)(a+b\xi)^*} = \sqrt{(a+b e^{i\frac{2\pi k}{3}})(a+b e^{-i\frac{2\pi k}{3}})} = a^2 + b^2 - ab(2\cos \frac{2\pi}{3}k) \quad k=1 \text{ or } 2.$$

$$\text{define } N(a+b\xi) = |a+b\xi|^2 = a^2 + b^2 - ab$$

then  $N(z_1 z_2) = N(z_1)N(z_2)$ . for any  $z_1, z_2$  whence if  $u = a+b\xi$ ,  $uv = 1$ . for some  $v \in R$ .

when  $N(u)N(v) = N(1) = 1$ . if  $ab \geq 0$ .  $a^2 + b^2 - ab \geq a^2 + b^2 - 2ab \geq 0$  if  $ab < 0$   $a^2 + b^2 - ab > 0$ .

We claim the equality of " $a^2 + b^2 - ab \geq a^2 + b^2 - 2ab \geq 0$ " can't holds simultaneously. thus  $a^2 + b^2 - ab \in \mathbb{Z}_+$

$\Rightarrow a^2 + b^2 - ab = 1. \Rightarrow (a, b) = (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1)$ . which involved the i/ case

$$\text{thus. } R^* = \{a+b\xi \mid (a, b) = (\pm 1, 0), (0, \pm 1), (\pm 1, \pm 1), \xi \neq 1\}.$$

Exercise 16.3. Consider the ring  $R = \mathbb{Z}[\sqrt{-3}]$  and prove that its ideal  $I = (2, 1+\sqrt{-3})$  is not principal.

Hint. It suffices to show that any common factor of 2 and  $1+\sqrt{-3}$  is a unit and  $I \neq R$ . Use  $N$  from Problem 16.5.

Pf. Assume  $I = (f)$  for some  $f \in \mathbb{Z}[\sqrt{-3}]$   $f \mid 2$  and  $f \mid 1+\sqrt{-3}$ .  $\exists h_1, h_2 \in R$ .  $2 = fh_1$   $1+\sqrt{-3} = fh_2$ .

$$\text{define } N: R \rightarrow \mathbb{Z} \quad N(a+b\sqrt{-3}) = |a+b\sqrt{-3}|^2 = a^2 + 3b^2.$$

$$N(f)N(h_1) = N(2) = 4 \quad \Rightarrow \quad N(f)N(h_1) = N(f)N(h_2) = 4$$

$$N(f)N(h_2) = N(1+\sqrt{-3}) = 4. \quad \text{by problem 6.5. we have } N(f), N(h_1), N(h_2) \in \mathbb{Z}_+.$$

and there is no integer  $a, b$  s.t.  $a^2 + 3b^2 = 2$ .

$$\text{thus } N(f) = 1 \quad N(h_1) = N(h_2) = 4 \quad \text{or} \quad N(f) = 4 \quad N(h_1) = N(h_2) = 1.$$

$$\text{If } N(f) = 4. \text{ we have } a^2 f + 3b^2 f = 4 \quad \text{①} \quad \begin{cases} af = \pm 2 \\ bf = 0 \end{cases} \quad \text{②} \quad \begin{cases} af = \pm 1 \\ bf = \pm 1 \end{cases} \quad \text{③} \quad \begin{cases} af = \pm 1 \\ bf = \mp 1 \end{cases}$$

$$\text{①. } h_1 = \pm 1. \text{ no } h_2 \in R. \text{ s.t. } 1+\sqrt{-3} = \pm 2 \cdot h_2. \quad \text{②. } h_2 = \pm 1. \text{ no } h_1 \in R. \text{ s.t. } \pm(1+\sqrt{-3})h_1 = 2.$$

③ no  $h_1$  and  $h_2 \in R$ . Thus.  $N(f) = 4$  is impossible.

Whence  $N(f) = 1$ .  $f = \pm 1$ . i.e. any common factor of 2 and  $1+\sqrt{-3}$  is a unit

We can claim that  $1 \notin I$ .  $\forall r_1, r_2 \in R$  consider.  $2r_1 + r_2(1+\sqrt{-3})$ .

$r_2(1+\sqrt{-3})$  be a complex number or an even integer, as well as  $2r_1$ .

thus.  $2r_1 + r_2(1+\sqrt{-3})$  can't result in an odd integer. i.e.  $1 \notin I$ . therefore  $I$  is not a principle.

# HW6

Exercise 17.1. Prove the distributivity of  $+$  and  $\cdot$  in  $R/I$ . Explain every equality you write.

Pf:  $\forall \bar{a}, \bar{b}, \bar{c} \in R/I$ . we need  $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$

$$\text{LHS} \stackrel{\textcircled{1}}{=} \bar{a} \cdot (\overline{b+c}) \stackrel{\textcircled{2}}{=} \overline{a(b+c)} \stackrel{\textcircled{3}}{=} \overline{ab+ac} \stackrel{\textcircled{4}}{=} \overline{ab} + \overline{ac} \stackrel{\textcircled{5}}{=} \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} = \text{RHS}.$$

$\textcircled{2}\textcircled{5}$  by def of multiplication.  $\textcircled{1}\textcircled{4}$  by def. of addition of quotient group.

$\textcircled{3}$  distributivity in ring  $R$ .

Exercise 17.2. Let  $k$  be a field,  $f \in k[t]$  be a reducible polynomial. Show that  $k[t]/(f)$  is not a field.

Pf: since  $f$  is reducible  $\exists h, g \in k[t] \setminus \{0\}$ , s.t.  $f = hg$ .  
 $\deg h, g \geq 1$ .  
thus  $\bar{f} = \bar{hg} = \bar{h} \cdot \bar{g}$ . in  $k[t]/(f)$ ,  $\bar{f} = 0$   
that is  $\bar{h} \cdot \bar{g} = 0$ . which means  $\bar{h}, \bar{g} \in k[t]/(f)$  but not have multiplication inverse.  
 $\rightarrow \bar{h} \neq 0, \bar{g} \neq 0$   
thus  $k[t]/(f)$  is not a ring.

Exercise 17.3. Prove that  $\mathbb{R}[t]/(f)$  is isomorphic to  $\mathbb{C}$  if  $f(t) = at^2 + bt + c$ , where  $a \neq 0, b, c \in \mathbb{R}$  and  $b^2 - 4ac < 0$ .

Hint. Follow the proof of Proposition 17.3. What will be the image of  $\bar{t}$  in this case?

Pf: define the mapping  $\varphi: \mathbb{R}[t]/(f) \rightarrow \mathbb{C}$  by  $\varphi(\bar{g}) = g\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right)$ .

the  $\varphi$  is well-defined, if  $f | g_1 - g_2$  then  $g_1(t) - g_2(t) = (a^2t^2 + bt + c)h(t)$  for some  $h \in \mathbb{R}[t]$ .

$$\text{whence } g_1\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right) - g_2\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right) = 0.$$

$$\text{Further } \varphi(\bar{g}_1 + \bar{g}_2) = \varphi\left(\overline{g_1 + g_2}\right) = (g_1 + g_2)\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right) = g_1\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right) + g_2\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right) = \varphi(\bar{g}_1) + \varphi(\bar{g}_2)$$

which implies  $\varphi$  preserves the addition. for multiplication, similarly.

by def.  $\varphi$  is surjective.

$$\text{if } \varphi(\bar{g}_1) = \varphi(\bar{g}_2) \text{ then, } h\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right) = 0 \text{ for } h = g_1 - g_2.$$

$$\text{then } h\left(\frac{-b - i\sqrt{4ac-b^2}}{2a}\right) = h\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right) = h\left(\frac{-b + i\sqrt{4ac-b^2}}{2a}\right) = 0$$

$$\text{thus } t - \frac{-b - i\sqrt{4ac-b^2}}{2a} \mid h \text{ and } t - \frac{-b + i\sqrt{4ac-b^2}}{2a} \mid h \text{ thus } at^2 + bt + c \mid h \Rightarrow \bar{g}_1 = \bar{g}_2.$$

whence  $\varphi$  is bijective. i.e.  $\mathbb{R}[t]/(t^2+1) \cong \mathbb{C}$ .

Exercise 17.4. Let  $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$  and  $I = (2+i)$ . Prove that  $R/I$  is isomorphic to  $\mathbb{Z}/5\mathbb{Z}$ .

Pf: denote a map:  $\varphi: R/I \rightarrow \mathbb{Z}/5\mathbb{Z} \quad \varphi(\overline{a+bi}) = \overline{2a+b}$

if.  $(2+i) | (a_1 + b_1 i) - (a_2 + b_2 i)$ .

$$\text{then } \varphi(\overline{a_1 + b_1 i}) - \varphi(\overline{a_2 + b_2 i}) = \overline{(a+bi)(2+i)} \text{ for some } a+bi \in R.$$

Whence  $\overline{2a_1 + b_1} - \overline{2a_2 + b_2} = \overline{(a+bi) \cdot 0} = \overline{0}$ . thus  $\varphi$  is correctly defined.

since  $\varphi(\overline{0}) = \overline{0} \quad \varphi(\overline{1}) = \overline{2} \quad \varphi(\overline{i}) = \overline{1} \quad \varphi(\overline{1+i}) = \overline{3} \quad \varphi(\overline{2}) = \overline{4}$ .  $\varphi$  is surjective.

if  $\varphi(\overline{a_1 + b_1 i}) = \varphi(\overline{a_2 + b_2 i})$ . then  $\overline{(a_1 - a_2) + (b_1 - b_2)i} = \overline{0}$  i.e.  $2(a_1 - a_2) + (b_1 - b_2) = 5k, k \in \mathbb{Z}$ .

by the parity. we have.  $\begin{cases} a_1 - a_2 = 2k \\ b_1 - b_2 = k \end{cases}$  for same  $k$ . thus.  $(2+i) | (a_1 - a_2) + (b_1 - b_2)i$ .

thus  $\overline{a_1 + b_1 i} = \overline{a_2 + b_2 i}$ .  $\Rightarrow \varphi$  is injective.

$\varphi$  is isomorphism. between  $R/I$  and  $\mathbb{Z}/5\mathbb{Z}$ .

Exercise 18.1. Prove that  $t^5 + \bar{2}t + \bar{1} \in \mathbb{Z}/3\mathbb{Z}[t]$  is irreducible.

Pf: denote  $f = t^5 + \bar{2}t + \bar{1}$

Assume the converse.  $\exists g \in \mathbb{Z}/3\mathbb{Z}[t]$  and  $\deg g \leq 2$ .  $g$  is monic. s.t.  $g \mid f$ .

firstly  $\deg g \neq 1$ . since  $f$  has no root (prop. 18.1).

$$g_1 = t^2 + \bar{1} \quad \text{has root.}$$

for  $\deg g = 2$ . we have following irreducible  $g_1 = \underline{t^2 + t + \bar{1}} \quad g_2 = t^2 + t + \bar{2} \quad g_3 = t^2 + \bar{2}t + \bar{2}$

(if  $g$  is reducible,  $\exists \deg h = 1$ . s.t.  $h \mid g$ . thus  $h \mid f$ . contradicts with  $f$  has no roots).

$$\begin{array}{r} t^3 - t^2 + \bar{1} \\ \hline t^2 + t + \bar{1} \mid \overline{t^5 + \bar{2}t + \bar{1}} \\ \hline t^5 + t^4 + t^3 \\ \hline - t^4 - t^3 \\ \hline - t^4 - t^3 - t^2 \\ \hline t^2 + \bar{2}t + \bar{1} \\ \hline t^2 + t + \bar{1} \\ \hline t \end{array} \quad \begin{array}{l} \text{thus. we have } f = g_1 (t^3 - t^2 + \bar{1}) + t. \text{ i.e. } g_1 \nmid f \\ \text{similarly. } f = g_2 (t^3 - t^2 - t) + t + \bar{1} \text{ i.e. } g_2 \nmid f \\ f = g_3 (t^3 - 2t^2 + t) + t + \bar{1} \text{ i.e. } g_3 \nmid f \\ \text{thus. there is no } g \text{ s.t. } g \mid f. \end{array}$$

Exercise 18.2. Prove that  $t^8 + t^7 + t^2 + t + \bar{1} \in \mathbb{Z}/2\mathbb{Z}[t]$  is irreducible.

(Pf: denote  $f = t^8 + t^7 + t^2 + t + \bar{1}$  and suppose  $g \mid f$ .  $g$  monic.  $g \in \mathbb{Z}[t]$  and  $\deg g \leq 4$ .

1) Suppose  $f = (t^4 + a_3 t^3 + a_2 t^2 + a_1 t + a_0)(t^4 + b_3 t^3 + b_2 t^2 + b_1 t + b_0)$ .

Since  $a_0 b_0 = \bar{1}$  we have  $a_0 = b_0 = \bar{1}$ .

$a_1 + b_1 = \bar{1}$  we have  $\begin{cases} a_1 = \bar{1} \\ b_1 = \bar{0} \end{cases}$  or  $\begin{cases} a_1 = \bar{0} \\ b_1 = \bar{1} \end{cases}$ . by the symmetry for  $a_i, b_i$  up to now. let  $\begin{cases} a_1 = \bar{1} \\ b_1 = \bar{0} \end{cases}$

$a_2 + b_2 = \bar{1}$ . i).  $\begin{cases} a_2 = \bar{1} \\ b_2 = \bar{0} \end{cases} \Rightarrow a_3 + b_3 = \bar{0} \Rightarrow$  i)  $\begin{cases} a_3 = \bar{1} \\ b_3 = \bar{1} \end{cases}$  or ii)  $\begin{cases} a_3 = \bar{0} \\ b_3 = \bar{0} \end{cases}$

i) impossible. there is  $t^6, t^3$  in  $f$ . ii) impossible. in that case  $t^7$  could not appear in  $f$ .

or ii)  $\begin{cases} a_2 = \bar{0} \\ b_2 = \bar{1} \end{cases} \Rightarrow a_3 + b_3 + \bar{1} = \bar{0} \Rightarrow$  iii)  $\begin{cases} a_3 = \bar{1} \\ b_3 = \bar{0} \end{cases}$  or iv)  $\begin{cases} a_3 = \bar{0} \\ b_3 = \bar{1} \end{cases}$

iii) impossible. there is  $t^6$  in  $f$  iv) impossible there is  $t^4$  in  $f$ . thus. case (1) is false.

2) Suppose.  $f = (t^4 + a_2 t^3 + a_1 t^2 + a_0)(t^4 + b_4 t^3 + b_3 t^2 + b_2 t^1 + b_1 t + b_0)$ .

$$f = t^8 + (a_2 + b_4)t^7 + (b_3 + a_1 b_4 + a_0)t^6 + (b_2 + a_2 b_3 + a_1 b_4 + a_0)b_4 t^5 + (b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4)t^4 \\ + (b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3)t^3 + (a_2 b_0 + a_1 b_1 + a_0 b_2)t^2 + (a_0 b_1 + a_1 b_0)t + a_0 b_0.$$

$$\left\{ \begin{array}{l} a_0 = b_0 = \bar{1} \\ a_2 + b_4 = \bar{1} \\ b_3 + a_1 = \bar{0} \\ a_1 + b_1 = \bar{1} \\ a_2 + b_2 = \bar{1} \end{array} \right. \begin{array}{l} \text{i) let } a_1 = \bar{0}. \text{ and by coe. of } t^4 \\ \Rightarrow b_1 = \bar{1} \\ b_3 = \bar{0} \\ a_2 = \bar{1} \\ b_2 = \bar{0} \end{array} \begin{array}{l} \text{but by coe. of } t^7 \\ b_1 + a_2 b_3 + a_1 b_4 + a_0 b_0 = \bar{0} \\ \Rightarrow \bar{1} + \bar{0} + \bar{0} + \bar{0} = \bar{0} \\ \Rightarrow b_4 = \bar{0} \end{array} \begin{array}{l} \text{contradicts.} \\ a_2 + b_4 = \bar{1} \\ \Rightarrow b_4 = \bar{1} \end{array}$$

ii) let  $a_1 = \bar{1}$  similarly. by coe. of  $t^4$  and  $t^7$  we have  $b_4 = \bar{1}$  and  $b_4 = \bar{0}$ . contradicts.

$\Rightarrow b_1 = \bar{0}$  thus  $a_1$  not exist. thus case (2) is impossible.

$$\begin{array}{l} b_3 = \bar{1} \\ b_2 = \bar{0} \\ a_2 = \bar{1} \end{array}$$

(3) Suppose  $\deg g = 2$  by problem 18.3.. it suffices to consider  $g = t^2 + 1$ .

$$\begin{array}{r} t^8 + t^7 + t^2 + t + 1 \\ \hline t^2 + t + 1 \quad | \quad t^8 + t^7 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1 \\ \hline t^8 + t^7 + t^6 \\ \hline -t^6 - t^5 - t^4 \\ \hline t^5 + t^4 + t^3 \\ \hline -t^5 - t^4 - t^3 \\ \hline t^4 + t^3 + t^2 + t \\ \hline -t^4 - t^3 - t^2 - t \\ \hline t^3 + t^2 + t \\ \hline -t^3 - t^2 - t \\ \hline t^2 + t + 1 \\ \hline -t^2 - t - 1 \\ \hline 2t^2 + 2t + 1 \\ \hline 2t^2 + 2t + 2 \\ \hline -1. \end{array} \begin{array}{l} \text{since. } -1 = \bar{1} \neq \bar{0} \\ \text{thus. } g \nmid f. \end{array}$$

(4).  $f$  has no roots. thus  $\deg g \neq 1$

In conclusion. there is no  $g$  satisfy the condition above. by Prop. 18.2.  $f$  is irreducible.

Exercise 18.3. Prove that  $f = 5t^5 + 4t^4 - 3t^2 + 9$  is irreducible over  $\mathbb{Z}$ .

Hint. Consider the reduction modulo 2 from  $\mathbb{Z}[t]$  to  $(\mathbb{Z}/2\mathbb{Z})[t]$ ,  $\varphi = \sum_{j=0}^n a_j t^j \mapsto \bar{\varphi} = \sum_{j=0}^n \bar{a}_j t^j$ .

Clearly  $\bar{\varphi}\bar{\psi} = \bar{\varphi}\bar{\psi}$ . Notice that  $\bar{f}$  is irreducible over  $\mathbb{Z}/2\mathbb{Z}$ .

Pf: consider mapping  $\Phi: \mathbb{Z}[t] \rightarrow (\mathbb{Z}/2\mathbb{Z})[t]$   $\varphi = \sum_{j=0}^n a_j t^j \mapsto \bar{\varphi} = \sum_{j=0}^n \bar{a}_j t^j$   
 $\deg \varphi \geq 1$

if  $f \in \mathbb{Z}[t]$  is reducible, let  $f = \varphi\psi$ .  $\varphi, \psi \in \mathbb{Z}[t]$ .  $\bar{f} = \bar{\varphi}\bar{\psi} = \bar{\varphi}\bar{\psi}$ . thus  $\bar{f}$  is reducible over  $\mathbb{Z}/2\mathbb{Z}$ .

thus it's. converse-negative proposition holds. i.e.  $\bar{f}$  is irreducible over  $\mathbb{Z}/2\mathbb{Z}$  implies  $f$  is irreducible over  $\mathbb{Z}$ .

$\bar{f} = t^5 + t^2 + \bar{1}$ . by Problem 18.3.  $\bar{f}$  is irreducible over  $\mathbb{Z}/2\mathbb{Z}$ .

**Exercise 19.1.** Construct a field of 8 elements. Write some non-evident entries of its Cayley tables.

Pf: prop 19.1 and 19.2. char k is prime p and  $|k| = p^n$ .

$p^n = 8 \Rightarrow$  the only possible case is  $p=2$ . and  $n=3$ .

By prop 19.3. we need to find  $\deg f = 3$ .  $f \in \mathbb{Z}/2\mathbb{Z}$ .  $f$  is irreducible.

(by prop 18.2)

let  $f = t^3 + t^2 + \bar{1}$  which has no roots and not divisible by  $t^2 + t + \bar{1}$ , thus it's irreducible over  $\mathbb{Z}/2\mathbb{Z}$ .

then we construct a field  $\mathbb{Z}/2\mathbb{Z}[t]/(t^3 + t^2 + \bar{1})$  of order 8.

$\{ \bar{0}, \bar{1}, \bar{t}, \bar{t} + \bar{1}, \bar{t}^2 + \bar{t} + \bar{1}, \bar{t}^2 + \bar{t}, \bar{t}^2 + \bar{1}, \bar{t}^3 \}$ . Some non-trivial entries:

$$(\bar{t}^2 + \bar{t})(\bar{t}^2 + \bar{1}) = \bar{t}^4 + \bar{t}^3 + \bar{t}^2 + \bar{t} = \bar{t}(\bar{t}^3 + \bar{t}^2 + \bar{1}) + \bar{t}^2 = \bar{t}^2.$$

$$(\bar{t}^2 + \bar{t} + \bar{1})(\bar{t}^2 + \bar{1}) = \bar{t}^4 + \bar{t}^3 + \bar{t} + \bar{1} = \bar{t}(\bar{t}^3 + \bar{t}^2 + \bar{1}) + \bar{1} = \bar{1}.$$

$$(\bar{t}^2 + \bar{t} + \bar{1})(\bar{t}^2 + \bar{t} + \bar{1}) = \bar{t}^4 + \bar{1} = \bar{t}(\bar{t}^3 + \bar{t}^2 + \bar{1}) + (\bar{t}^3 + \bar{t}^2 + \bar{1}) + \bar{t}^2 + \bar{t} = \bar{t}^2 + \bar{t}.$$

$$(\bar{t}^2 + \bar{t} + \bar{1})(\bar{t}^2 + \bar{t}) = \bar{t}^4 + \bar{t} = \bar{t}(\bar{t}^3 + \bar{t}^2 + \bar{1}) + (\bar{t}^3 + \bar{t}^2 + \bar{1}) + \bar{t}^2 + \bar{1} = \bar{t}^2 + \bar{1}$$

$$(\bar{t}^2 + \bar{t} + \bar{1}) + (\bar{t}^2 + \bar{t}) = \bar{1}$$

$$(\bar{t}^2 + \bar{t} + \bar{1}) + \bar{t}^2 = \bar{t} + \bar{1}$$

**Exercise 19.2.** Let  $f(x) = x^3 - x + \bar{1} \in \mathbb{Z}/3\mathbb{Z}[x]$ . Using the representation of the elements of the field  $\mathbb{Z}/p\mathbb{Z}[x]/(f)$  as  $a\bar{x}^2 + b\bar{x} + c$ ,  $a, b, c \in \mathbb{Z}/3\mathbb{Z}$ , find  $(\bar{x}^2 + \bar{1})^{-1}$ .

Hint. Follow the proof of Proposition 17.2.

Solution: Consider  $f = x^3 - x + \bar{1} = x^3 + \bar{2}x + \bar{1}$ .  $g = x^2 + \bar{1}$ .

$g \nmid f$ . thus  $\gcd(f, g) = \bar{1}$  by Bezout's identity.  $\exists h_1, h_2 \in \mathbb{Z}/3\mathbb{Z}[t]$ .  $h_1 f + h_2 g = \bar{1}$

find  $h_1 = 2(\bar{1} - x)$   $h_2 = \bar{2}(x^2 - x + \bar{1})$

$$h_1 f + h_2 g = \bar{2}(\bar{1} - x)(x^3 + \bar{2}x + \bar{1}) + \bar{2}(x^2 - x + \bar{1})(x^2 + \bar{1}) = \bar{2} [x^3 + \bar{2}x + \bar{1} - x^4 - \bar{2}x^2 - x + x^4 + x^2 - x^3 - x + x^2 + \bar{1}] = \bar{2} \cdot \bar{2} = \bar{1}.$$

in  $\mathbb{Z}/3\mathbb{Z}[t]/f$ .  $\bar{h}_2 \cdot \bar{g} = \bar{h}_2 \bar{g} = \bar{1}$ .  $\bar{g}$  has inverse  $\bar{h}_2$ . i.e.  $(\bar{x}^2 + \bar{1})^{-1} = \bar{x}$ .

HW7.

Exercise 20.1. Let  $F = \mathbb{Z}/3\mathbb{Z}[t]/(t^3 - t + 1)$ . Find the minimal polynomial for  $\bar{t}^2 \in F$  over  $\mathbb{Z}/3\mathbb{Z}$ .

$$\text{Pf: denote } \alpha = \bar{t}^2. \quad \alpha^3 = \bar{t}^4 = \overline{t(t^3-t+1)+t^2-t} = \overline{\bar{t}^2-\bar{t}} = \overline{\bar{t}^2+2\bar{t}}$$

$$\alpha^3 = \overline{t^2(t^2+2t)} = \overline{t^4} + \overline{2t^3} = \overline{\bar{t}^2+2\bar{t}} + \overline{2(t^3-t+1)+2t-2} = \overline{\bar{t}^2+t+1}$$

$$\text{Now. } a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = \bar{0}$$

$$\Rightarrow \begin{cases} a_3 + a_0 = \bar{0} \\ a_3 + 2a_2 = \bar{0} \\ a_3 + a_2 + a_1 = \bar{0} \end{cases} \Rightarrow \text{non-trivial sol.} \quad a_1 = a_2 = a_3 = \bar{1}, \quad a_0 = \bar{2}$$

$$\text{thus the minimal poly } f(x) = x^3 + x^2 + x + \bar{2}$$

Exercise 21.1. Prove that  $\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(i\sqrt[3]{2})$ .

$$\text{Pf: let } \alpha = i\sqrt[3]{2}. \quad \alpha^3 = -2i \quad \alpha^6 = 2. \quad \text{one has } i = -\frac{1}{2}\alpha^3 \quad \sqrt[3]{2} = -i\alpha = \frac{1}{2}\alpha^4$$

Now  $\mathbb{Q}(i\sqrt[3]{2})$  is a field contain  $\sqrt[3]{2}$ , and  $i$ . for any extension  $L/\mathbb{Q}$  with  $i$  and  $\sqrt[3]{2}$  one has  $\mathbb{Q}(i\sqrt[3]{2})$ . by uniqueness. of the generating extension.  $\mathbb{Q}(i\sqrt[3]{2}) = \mathbb{Q}(i, \sqrt[3]{2})$ .

Exercise 21.2. Show that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$ .

$$\text{Pf: let } \alpha = \sqrt{2} + \sqrt{3}. \quad \alpha^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6} \quad \sqrt{6} = \frac{\alpha^2 - 5}{2}$$

$$\text{let } \beta = \sqrt{3} - \sqrt{2}. \quad \beta^2 = 5 - 2\sqrt{6}. \quad \sqrt{2} = \frac{\alpha + \beta}{2} \quad \sqrt{3} = \frac{\alpha - \beta}{2}$$

clearly.  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha, \beta)$  (by problem 21.5).

$\mathbb{Q}(\alpha, \beta)$  is a field contains.  $\sqrt{2}, \sqrt{3}, \sqrt{6}$ . and  $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$

by the uniqueness of extension.  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha, \beta) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\}$ .

Exercise 21.3. Remove the irrationality in the denominator in  $\frac{1}{1+\sqrt{2}+\sqrt{3}-\sqrt{6}}$ .

Sol:  $\alpha = 1 + \sqrt{2} + \sqrt{3} - \sqrt{6}$ . find  $f \in \mathbb{Q}[t]$  s.t.  $f(\alpha) = 0$

$$\alpha^2 = 1 + 2 + 3 + 6 + 2\sqrt{2} + 2\sqrt{3} - 2\sqrt{6} - 4\sqrt{3} + 2\sqrt{6} - b\sqrt{2}$$

$$= 12 - 4\sqrt{2} - 2\sqrt{3}.$$

$$\alpha^3 = (12 - 4\sqrt{2} - 2\sqrt{3})(1 + \sqrt{2} + \sqrt{3} - \sqrt{6}) = -2 + 14\sqrt{2} + 18\sqrt{3} - 18\sqrt{6}$$

$$\text{assume } a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = 0$$

$$\begin{cases} -2a_3 + 12a_2 + a_1 + a_0 = 0 \\ 14a_3 - 4a_2 + a_1 = 0 \\ 18a_3 - 2a_2 + a_1 = 0 \\ -18a_3 - a_1 = 0 \end{cases} \Rightarrow \begin{cases} a_3 = 0 \\ a_2 = 0 \\ a_1 = 0 \\ a_0 = 0 \end{cases} \text{only trivial solution?}$$

**Exercise 21.4.** Find the minimal polynomial of  $\alpha = \sqrt{2} + \sqrt[3]{3}$  over  $\mathbb{Q}$ . Don't forget to prove its minimality.

*Hint.* Since  $\mathbb{Q}(\sqrt{2})$  and  $\mathbb{Q}(\sqrt[3]{3})$  are subfields of  $\mathbb{Q}(\alpha)$ , the degree of the minimal polynomial for  $\alpha$  over  $\mathbb{Q}$  must be at least 6.

Pf:  $\alpha = \sqrt{2} + \sqrt[3]{3}$ .

$\mathbb{Q}(\sqrt{2})$  has deg 2. over  $\mathbb{Q}$ .  $\mathbb{Q}(\sqrt[3]{3})$  has deg 3.

thus.  $\mathbb{Q}(\alpha)$  has deg. at least 6.

$$\alpha - \sqrt{2} = \sqrt[3]{3} \Rightarrow (\alpha - \sqrt{2})^3 = 3 \Rightarrow \alpha^3 + b\alpha - 3 = (3\alpha^2 + b)\sqrt{2} \Rightarrow (\alpha^3 - b\alpha - 3)^2 = 18(\alpha^2 + 2)^2$$

$$\Rightarrow \alpha^6 + 12\alpha^4 + 3b\alpha^2 - b\alpha^3 - 3b\alpha + 9 = 18\alpha^4 + 72\alpha^2 + 72 \Rightarrow \alpha^6 - b\alpha^4 - 3b\alpha^2 - b\alpha^3 - 3b\alpha - 63 = 0$$

thus  $f(\alpha) = \alpha^6 - b\alpha^4 - 3b\alpha^2 - 3b\alpha - 63$ .  $f(\alpha)$ . deg 6. irreducible. over  $\mathbb{Q}$ . thus it's minimal.

**Exercise 22.1.** Prove that a regular heptagon can not be constructed using a compass and an straightedge.

$$\cos \frac{2\pi}{7}$$

*Hint.* Show that  $\alpha = 2 \cos \frac{2\pi}{7}$  is not a constructible number by finding its minimal polynomial.

Pf: the central angle of regular heptagon is  $\frac{2\pi}{7}$ .

$$\cos(7\theta) = 64\cos^7\theta - 112\cos^5\theta + 56\cos^3\theta - 7\cos\theta = 0.$$

$$\Rightarrow f(t) = 64t^7 - 112t^5 + 56t^3 - 7t = t(64t^6 - 112t^4 + 56t^2 - 7)$$

$\Rightarrow t=0$  is not the required sol. w.r.t. cos. Let  $x = t^2$ .

$$\Rightarrow g(x) = 64x^3 - 112x^2 + 56x - 7 \quad g(x) \text{ is irreducible over } \mathbb{Q}.$$

thus. the deg.  $\mathbb{Q}(\cos \frac{2\pi}{7})$ . = 3.  $\neq 2^n$  thus. by prop. 22.5.  $\cos(\frac{2\pi}{7})$  not constructible number.