Homework 1.

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

Pf: $(a*b)*c = c*(a*b)$ by commutative of $*$

$= c*(b*a)$ by commutative again.

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

i.e. $a+b+ab = 0$ 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 $\mathbb{Z}/4\mathbb{Z}$*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1) closeness. since $g_2, g_1 \in G$. $g_1 \bullet g_2 = g_2 * g_1 \in G$ (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 $*$)

$= (g_2 * g_1) \bullet g_3 = (g_1 \bullet g_2) \cdot g_3$ (by def. operation $\bullet$)

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

$e \bullet g_1 = g_1 * e = g_1$. $\quad g_1 \bullet e = e * g_1 = e$

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. $*$)

$g_1 \bullet g_1' = g_1' * g_1 = e$ $\quad g_1' \bullet g_1 = g_1 * g_1' = e$ 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 $F = \{f(t) \mid \frac{at+b}{ct+d}, a, b, c, d \in \mathbb{R}. ad-bc \neq 0\}$.

$\forall\ f_1(t) = \frac{a_1 t + b_1}{c_1 t + d_1} \quad f_2(t) = \frac{a_2 t + b_2}{c_2 t + d_2} \in F.$

1) $f_1(f_2(t)) = \frac{(a_1 a_2 + b_1 c_2)t + (a_1 b_2 + b_1 d_2)}{(c_1 a_2 + d_1 c_2)t + (c_1 b_2 + d_1 d_2)}$

$(a_1 a_2 + b_1 c_2)(c_1 b_2 + d_1 d_2) - (c_1 a_2 + d_1 c_2)(a_1 b_2 + b_1 d_2) = a_1 a_2 d_1 d_2 + b_1 b_2 c_1 c_2 - a_2 b_1 c_1 d_2 - a_1 c_2 b_2 d_1$

$= a_1 d_1 (a_2 d_2 - c_2 d_2) + b_1 c_1 (b_2 c_2 - a_2 d_2) = (a_1 d_1 - c_1 b_1)(a_2 d_2 - c_2 b_2) \neq 0.$ 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) $\forall f = \frac{at+b}{ct+d} \in F.$

$\exists f^{-1} = \frac{dt-b}{-ct+a} \in F.$ s.t. $f^{-1}(f(t)) = \frac{d(\frac{at+b}{ct+d}) - b}{-c(\frac{at+b}{ct+d}) + a} = \frac{dat - cbt}{-cb + ad} = t.$ 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) $\{\overline{1}, \overline{9}\}$
ii) $\{\overline{1}, \overline{7}\}$
iii) $\{\overline{1}, \overline{3}, \overline{7}\}$
iv) $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$

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. $\overline{1}$ is the identity element.

(1) A_1 is a group.

① operation is closed. $\overline{1}\cdot\overline{1} = \overline{1} \in A_1 \quad \overline{1}\cdot\overline{9} = \overline{9} \in A_1 \quad \overline{9}\cdot\overline{9} = \overline{1} \in A_1$

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

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

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

(2) A_2 not group.

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

(3). A_3 not a group

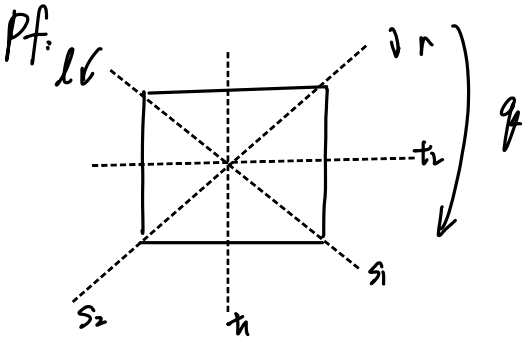
the operation is not closed since $\overline{3}\cdot\overline{3} = \overline{9} \notin A_3.$

(4) A_4 not a group.

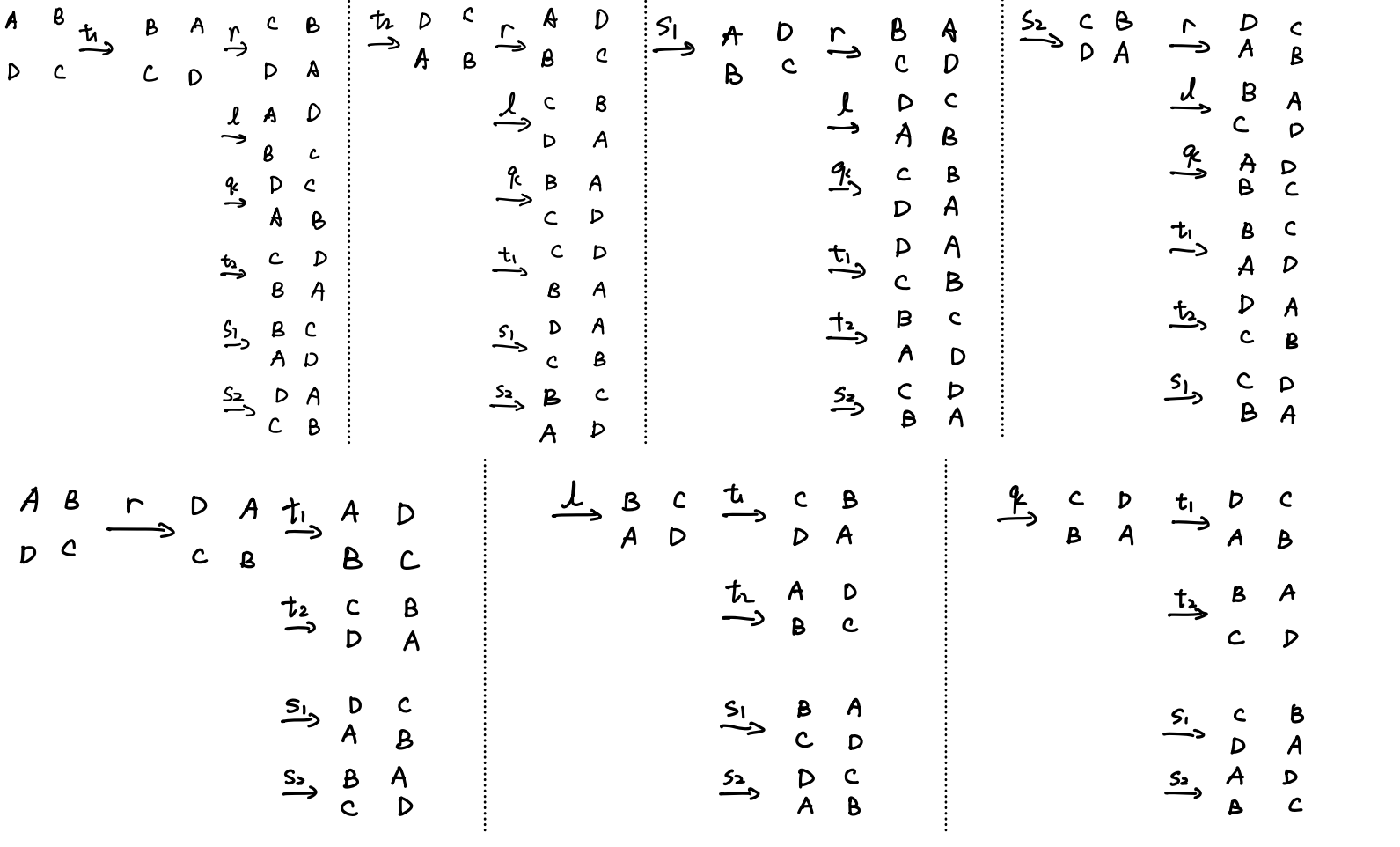
same as (3)

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 $90°$, l is the counterclockwise rotation about O by $90°$, q be the rotation about O by $180°$ (= 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 $D_4 = \{e, r, l, q, t_1, t_2, s_1, s_2\}$.*

Pf:



	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



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

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

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

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

① the operation is closed.

② b is the identity elements.

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

④ i/ if one of $e_i = b$, 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.

$\forall\ e_1, e_2, e_3 \in G$, 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

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

iv/ check the remaining case:

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

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

thus, the operation is associative.

(2) $B = \{a, b, c, d, e\}$. 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* $\{A \in \mathrm{M}_n(\mathbb{R}) \mid AA^T = E_n\}$ *form a subgroup of* $\mathrm{GL}_n(\mathbb{R})$.

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

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

$A_1A_2(A_1A_2)^T = A_1 A_2 A_2^T A_1^T = A_1 E_n A_1^T = E_n$. thus $A_1A_2 \in H$

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

$A^T \cdot (A^T)^T = A^T \cdot A = A^{-1} \cdot A = E_n$, 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. $h * h^{-1} = h^{-1} * h = e$. $h' * h'^{-1} = h'^{-1} * h' = e$

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

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

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

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

$\bar{0}$ has inverse $\bar{0}$. $\bar{2}$ has inverse $\bar{4}$.

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

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

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

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

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

if one of $|a_i|>1$. $\lim_{m\to\infty}|a_i|^m = +\infty$ 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 Ex4.4

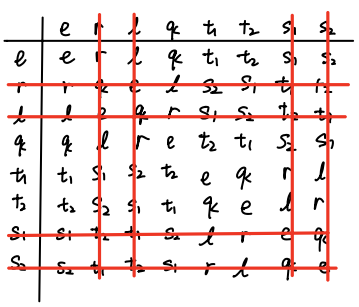
	e	r	l	q	t_1	t_2	s_1	s_2
e	e	r	l	q	t_1	t_2	s_1	s_2
r	r	q	e	l	s_2	s_1	t_1	t_2
l	l	e	q	r	s_1	s_2	t_2	t_1
q	q	l	r	e	t_2	t_1	s_2	s_1
t_1	t_1	s_1	s_2	t_2	e	q	r	l
t_2	t_2	s_2	s_1	t_1	q	e	l	r
s_1	s_1	t_2	t_1	s_2	l	r	e	q
s_2	s_2	t_1	t_2	s_1	r	l	q	e

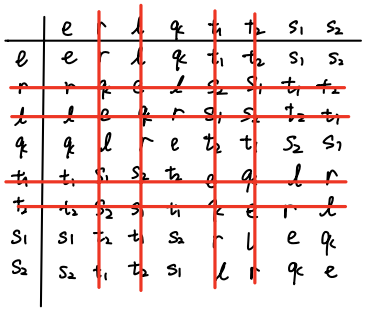
by the table

$\{e, r, l, q\}$ → block the table.

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

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





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

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

Pf: denote ord $gh = m$.

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

$\Rightarrow g*(h*g)^{m-1}*h = e$. 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 ord hg = ord gh = m.

2) if $m = +\infty$. i.e. $(gh)^m \neq e$ for any m.

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

thus. ord $hg = +\infty$.

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

Hint. Use Proposition 6.3.

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

$(g^s)^{\frac{n}{d}} = g^{\frac{ns}{d}}$ (by prop. 6.1)

$= (g^n)^{\frac{s}{d}}$ (by prop. 6.1)

$= e^{\frac{s}{d}} = e$. (since. $d = \gcd(n,s)$. $d \mid s$. $\frac{s}{d} \in \mathbb{Z}$.)

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

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

by prop. 6.3. we have $A \mid \frac{n}{d} \Rightarrow At_1 = \frac{n}{d}$ for some integer $t_1 \neq 1$.

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

thus $SA = tn$ for some integer $t_2 \neq 1$. i.e. $A = \frac{t_2 n}{s}$.

$\begin{cases} A = \frac{t_2 n}{s} \\ At_1 = \frac{n}{d} \end{cases} \Rightarrow \frac{t_2 n}{s} = \frac{n}{t_1 d} \Rightarrow s = t_1 t_2 d$. that is. $\begin{cases} n = t_1 d\, n \\ s = t_1 d\, t_2 \end{cases}$ we have $t_1 d > d$

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

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	l_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 $He = Hs_1 = \{e, s_1\}$

$rH = t_1 H = \{re, rs_1\} = \{r, t_1\}$. $Hr = Ht_2 = \{er, s_1 r\} = \{r, t_2\}$

$lH = t_2 H = \{le, ls_1\} = \{l, t_2\}$ $Hl = Ht_1 = \{el, s_1 l\} = \{l, t_1\}$

$qH = s_2 H = \{q, s_2\}$. $Hq = Hs_2 = \{eq, s_1 q\} = \{q, s_2\}$

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 $H = \{A \in GL_n(\mathbb{C}) \mid \det A \in \mathbb{R}\}$.

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

$\forall A \in GL_n(\mathbb{C})$. if $A \in H$. then $AH = HA = H$.

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

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

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

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.

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

since $h \in H \sqsubset H_1$. H_1 is normal. $gH_1 = H_1 g$. $hg \in gH_1$

since $h \in H \sqsubset H_2$ H_2 is normal. $gH_2 = H_2 g$. $hg \in gH_2$ $\Rightarrow$ $hg \in gH$.

since h is arbitrary. $Hg \sqsubset gH$.. similarly, $Hg \sqsupset gH$. 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 $H_n^m = \{\sigma \in S_n \mid \sigma(m) = m\}$.

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

let $g = (213)$. $gH_3^2 = \{(231), (312)\}$ $H_3^2 g = \{(213), (231)\}$

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

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.*

i) *Prove that the relation $\sim$ on G is an equivalence relation*

ii) *Find the partition of $G = D_3, D_4$ into the equivalence classes*

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

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

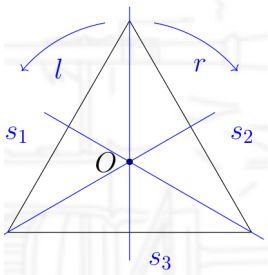
. since G is a group. $g^{-1} \in G$ and $(g^{-1})^{-1} = g$. $g_2 \sim g_1$.

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

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

ii) for D_3. we have the table.

	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



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

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

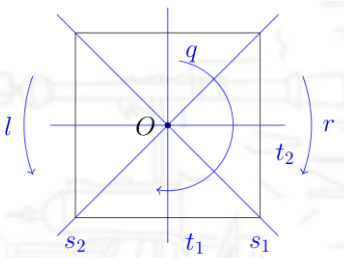
$s_1 s_3 s_1^{-1} = s_1 s_3 s_1 = l s_1 = s_2$ $s_2 \sim s_3$.

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

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_2	t_1
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



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

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

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

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

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 $|H_1| = 15, |H_2| = 28$.*

i) *Find the minimum possible order of G.*

ii) *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. $|H_1| = |H| \cdot |H_1 : H|$

$|H_2| = |H| \cdot |H_1 : H|$.

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* $H = \{x, \bar{3}x, \bar{9}x\}$, $H' = \{\pm x, \pm\bar{3}/x\}$.

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

$(ax)\cdot(bx) = abx$

$(ax)\cdot(b/x) = ab/x$

$(a/x)\cdot(b/x) = ab^{-1}x$

$(a/x)\cdot(bx) = ab^{-1}/x$.

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

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

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

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

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

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

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

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

$ghg^{-1} \in H$. $b \in H$

use lemma 7.3. $(ax)\cdot(bx)\cdot(ax)^{-1} = (aba^{-1})x = bx \in H$

$(a/x)(bx)(a/x)^{-1} = (a/x)(b^a/x) = \bar{b}^1 x \in H$.

$(ax)^{-1} = a^{-1}x$. $(a/x)^{-1} = a/x$.

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

$\alpha = 1$. $Hg_1 = \{a_1x, \bar{3}\cdot a_1x, \bar{9}\cdot a_1x\}$.

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

thus $Hg_1 = g_1H$.

$\alpha = -1$. $g_1H = \{a_1x^{-1}, \frac{a_1}{3}x^{-1}, \frac{a_1}{9}x^{-1}\} = \{a_1x^{-1}, \bar{9}a_1x^{-1}, \bar{3}a_1x^{-1}\}$

$Hg_1 = \{a_1x^{-1}, \bar{3}a_1x^{-1}, \bar{9}a_1x^{-1}\} = Hg_1$. thus $H \triangleleft G$.

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

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

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

iv)

	$x\cdot H$	$\bar{2}x\cdot H$	$\bar{4}x\cdot H$	$\bar{7}x\cdot H$	$x^{-1}\cdot H$	$\bar{2}x^{-1}\cdot H$	$\bar{4}x^{-1}\cdot H$	$\bar{7}x^{-1}\cdot H$
$x\cdot H$	$x\cdot H$	$\bar{2}x\cdot H$	$\bar{4}x\cdot H$	$\bar{7}x\cdot H$	$x^{-1}\cdot H$	$\bar{2}x^{-1}\cdot H$	$\bar{4}x^{-1}\cdot H$	$\bar{7}x^{-1}\cdot H$
$\bar{2}x\cdot H$	$\bar{2}x\cdot H$	$\bar{4}x\cdot H$	$\bar{7}x\cdot H$	$x\cdot H$	$\bar{2}x^{-1}H$	$\bar{4}x^{-1}H$	$\bar{7}x^{-1}\cdot H$	$x^{-1}\cdot H$
$\bar{4}x\cdot H$	$\bar{4}x\cdot H$	$\bar{7}x\cdot H$	$x\cdot H$	$\bar{2}xH$	$\bar{4}x^{-1}H$	$\bar{7}x^{-1}H$	$x^{-1}\cdot H$	$\bar{2}x^{-1}\cdot H$
$\bar{7}x\cdot H$	$\bar{7}x\cdot H$	$x\cdot H$	$\bar{2}x\cdot H$	$\bar{4}x\cdot H$	$\bar{7}x^{-1}H$	$x^{-1}H$	$\bar{2}x^{-1}\cdot H$	$\bar{4}x^{-1}\cdot H$
$x^{-1}\cdot H$	$x^{-1}\cdot H$	$\bar{7}x^{-1}\cdot H$	$\bar{4}x^{-1}H$	$\bar{2}x^{-1}H$	$x\cdot H$	$\bar{7}xH$	$\bar{4}x\cdot H$	$\bar{2}x\cdot H$
$\bar{2}x^{-1}\cdot H$	$\bar{2}x^{-1}\cdot H$	$x^{-1}\cdot H$	$\bar{7}x^{-1}\cdot H$	$\bar{4}x^{-1}\cdot H$	$\bar{2}x\cdot H$	xH	$\bar{7}x\cdot H$	$\bar{4}x\cdot H$
$\bar{4}x^{-1}\cdot H$	$\bar{4}x^{-1}\cdot H$	$\bar{2}x^{-1}\cdot H$	$x^{-1}\cdot H$	$\bar{7}x^{-1}\cdot H$	$\bar{4}x\cdot H$	$\bar{2}xH$	$x\cdot H$	$\bar{7}x\cdot H$
$\bar{7}x^{-1}\cdot H$	$\bar{7}x^{-1}\cdot H$	$\bar{4}x^{-1}\cdot H$	$2x^{-1}\cdot H$	$x^{-1}\cdot H$	$\bar{7}x\cdot H$	$\bar{4}xH$	$\bar{2}x\cdot H$	$x\cdot H$

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 $K(G) \subseteq H$. 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 $K(S_4) \subseteq A_4$

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 $|B_4| = 8$, $|C_4| = 3$, $|\{e\}| = 1$.

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 $B_4 \subseteq K(S_4)$.

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. $C_4 \subseteq K(S_4)$, then we have $A_4 \subseteq K(S_4)$. 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: $\begin{cases} ax \circ a'x = aa'x \\ b/x \circ b'/x = bb'^{-1}x \\ ax \circ b/x = ab\,x^{-1} \\ b/x \circ ax = b/(ax) = b\cdot a^{-1}\cdot x^{-1} \end{cases}$

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. $K(G) \trianglelefteq A$.

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

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

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

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

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

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

$\bar{9}\cdot\bar{9} = \bar{3}$ $\bar{10}\cdot\bar{10} = \bar{9}$ $\bar{11}\cdot\bar{11} = \bar{4}$ $\bar{12}\cdot\bar{12} = \bar{1}$

$-\bar{6} = \bar{7}$ $-\bar{5} = \bar{8}$ 不用再算了.

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 $\varphi: \mathbb{R}^* \to \mathbb{R}^*$ $\varphi(x) = x^2$ is a homomorphism. Find its image and kernel.

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

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

$e_{\mathbb{R}^*} = 1.$ let $\varphi(x) = 1 \Rightarrow x^2 = 1 \Rightarrow x = \pm 1$ $\ker\varphi = \{\pm 1\}$.

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

Exercise 10.3. *Let $\varphi \in \mathrm{Hom}(G, G')$.*

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

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

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

$\forall h \in H$, $\exists h' \in H'$ 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. $\varphi(g) \cdot \varphi(g)^{-1} \in G'$.

since $H' \triangleleft G'$. for all $h' \in H'$. $g' \in G'$ $g'h'g'^{-1} \in H'$. (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). $\mathrm{Im}(\varphi) < G'$ 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 $\varphi(\bar{1}) = a$. $\varphi \in \mathrm{End}(\mathbb{Z}/6\mathbb{Z})$.

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

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

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

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

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

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

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

⑤ $\varphi(\bar{1}) = \bar{4}$ endomorphism φ:

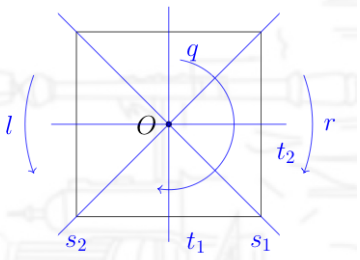
x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\varphi(x)$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$

⑥ $\varphi(\bar{1}) = \bar{5}$ endomorphism φ:

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

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 alway exists. $\varphi(x) = \bar{0}$. $x \in D_4$.

2) find nontrivial homomorphism.

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

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

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

thus $\varphi(q) = \bar{0}$.

$t_1 = t_2 q$. $s_1 = s_2 q$ $r = lq \Rightarrow \varphi(s_1) = \varphi(s_2)$ $\varphi(t_1) = \varphi(t_2)$. $\varphi(r) = \varphi(l)$

$s_1 s_2 = q$ $t_1 t_2 = q$ $rl = q \Rightarrow 2\varphi(s_1) = 2\varphi(t_1) = 2\varphi(r) = \bar{0} \to$ their $= \bar{3}$ or $\bar{0}$.

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

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

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

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

In conclusion. homomorphism define as:

1).

x	e	r	l	q	t_1	t_2	s_1	s_2
$\varphi(x)$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$

2)

x	e	r	l	q	t_1	t_2	s_1	s_2
$\varphi(x)$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{3}$	$\bar{3}$	$\bar{3}$

3)

x	e	r	l	q	t_1	t_2	s_1	s_2
$\varphi(x)$	$\bar{0}$	$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{0}$

4)

x	e	r	l	q	t_1	t_2	s_1	s_2
$\varphi(x)$	$\bar{0}$	$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{3}$	$\bar{3}$

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 $G = \langle a, b \rangle$.

$\forall g \in G$. $g = a^{Ng_1} b^{Ng_2}$, $Ng_1, Ng_2 \in \mathbb{Z}$.

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

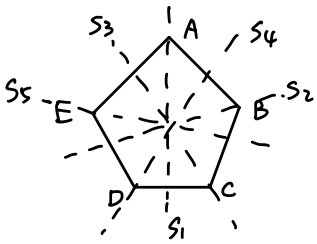
i.e. $h = \varphi(a^{Ng_1} b^{Ng_2}) = \varphi(a^{Ng_1}) * \varphi(b^{Ng_2}) = \varphi(a)^{Ng_1} * \varphi(b)^{Ng_2}$.

since h is arbitrary, $H = \langle \varphi(a), \varphi(b) \rangle$

Exercise 11.2. *Prove that* $D_3 \times \mathbb{Z}/5\mathbb{Z} \ncong D_5 \times \mathbb{Z}/3\mathbb{Z}$

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_5. $l, r, 2l, 2r$ has order 5. s_1, s_2, s_3, s_4, s_5 has order 2.

in $\mathbb{Z}/3\mathbb{Z}$ order is 1, 3, 3.

by def. of order, $\operatorname{ord}(h \times g) = \operatorname{lcm}(\operatorname{ord} h, \operatorname{ord} g)$.

in $D_3 \times \mathbb{Z}/5\mathbb{Z}$ $\exists\ s_1 \times \bar{1}$. 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* $\mathbb{Q} \ncong \mathbb{Q} \times \mathbb{Q}$

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

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

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

Assume. φ: $G \to G'$ - isomorphic.

$\forall\ \varphi(g_1), \varphi(g_2) \in G'$. $\exists g$. $g_1 = g^n$. $g_2 = g^m$. $\Rightarrow$ $\varphi(g_1) = \varphi(g^n) = \varphi(g)^n$

$\varphi(g_2) = \varphi(g^m) = \varphi(g)^m$.

i.e. $\exists\ \varphi(g)$. $\varphi(g_1) = \varphi(g)^n$, $\varphi(g_2) = \varphi(g^m)$.

isomorphism preserve this property.

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

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

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

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

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

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

$\varphi(\frac{p}{q}) = p \cdot \varphi(\frac{1}{q}) = \frac{p}{q}(a,b)$. 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. $\varphi(\frac{p_1}{q_1}) = (a, b+1)$.

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 φ is not bijective.

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

thus $\mathbb{Q} \ncong \mathbb{Q} \times \mathbb{Q}$

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

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

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

since $(i)^4 = (-i)^4 = (1)^4 = (-1)^4 = 1 = e_{\mathbb{C}^*}$. $\ker \varphi = H$.

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

$\forall A, B \in G$. $\varphi(AB) = \left(\frac{\det AB}{|\det AB|}\right)^4 \cdot |\det AB| = \left(\frac{\det A}{|\det A|}\right)^4 \cdot \left(\frac{\det B}{|\det B|}\right)^4 \cdot |\det A| \cdot |\det B|$

$= \left[\left(\frac{\det A}{|\det A|}\right)^4 |\det A|\right] \cdot \left[\left(\frac{\det B}{|\det B|}\right)^4 \cdot |\det B|\right] = \varphi(A) \cdot \varphi(B)$., i.e. $\varphi \in \operatorname{Hom}(G, H)$

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

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 $\operatorname{ord} a = 4$ 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 $\exists a$, $\operatorname{ord} a = 8$. then $\langle a \rangle = G$. G is cyclic group. thus $G \cong \mathbb{Z}/8\mathbb{Z}$. by thm 12.1.

ii) if $\operatorname{ord} a_i = 2$ 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. $e_i \mapsto \bar{0}$ $a_i \mapsto \bar{1}$ (in i th place.)

iii) if there exists $\operatorname{ord} a = 4$, 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 cancelation law of group and $a \neq b \neq e$. the elements are distinct. $|G| = 8$.

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

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

and φ 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 $\operatorname{ord} g = p$ 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.

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

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

$a \cdot (b \cdot g_1) = a(g_1^b) = (g_1)^{ba} = (g_1)^{ab} = (a \cdot b) \cdot g_1$ by prop 6.1. and commutivity 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. $\{g_i\}_{i\in[1:n]}$.

$\forall\, g\in G.\ \exists\,\{\varepsilon_1,\dots\varepsilon_n\}\ \ \varepsilon_i\in\mathbb{Z}/p\mathbb{Z}$ s.t. $g=\sum\varepsilon_i g_i$ 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. $\{e_i\}_{i\in[1:n]}$ $e_i=(\bar0,\dots,\bar1,\dots\bar0)$ $\bar1$ appears in ith place.

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

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

$\varphi:\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}\times\cdots\times\mathbb{Z}/p\mathbb{Z}.\to G$ s.t. $\varphi(a)=\varphi(\sum a_ie_i)=\sum a_i\varphi(e_i)=\sum a_ig_i=g$

And since $\varphi(a)\varphi(b)=\varphi(\sum a_ie_i)\varphi(\sum b_ie_i)=\sum(a_ib_i)\varphi(e_i)=\varphi(ab)$.

$\varphi\in\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}\times\cdots\times\mathbb{Z}/p\mathbb{Z}.,G)$. 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 $G_{m'}=gG_mg^{-1}$ for some $g\in G$.

Pf: m, m' belongs to the same orbit. i.e. $\exists\, g_0\in G$ s.t. $m'=g_0m$ $\exists\, g_1\in G$ s.t. $m=g_1m'$

$\forall\, h\in G_m$. consider conjugation $h'=g_0hg_0^{-1}$

$h'm'=g_0hg_0^{-1}m'=g_0hg_0^{-1}\cdot g_0\cdot m=g_0(hm)=g_0m=m'$. thus $h'\in G_{m'}$

$\forall\, h'\in G_{m'}$ consider conjugation $h=g_1h'g_1^{-1}$

$hm=g_1h'g_1^{-1}m=g_1h'g_1^{-1}\cdot g_1m'=g_1h'm'=g_1m'=m$ thus $h\in G_m$.

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

denote map $\varphi:G_m\to G_{m'}$. $\varphi(h)=g_0hg_0^{-1}$

$\forall\, h_1,h_2\in G_m$ $\varphi(h_1)\varphi(h_2)=g_0h_1(g_0^{-1}\cdot g_0)h_2g_0^{-1}=g_0(h_1h_2)g_0^{-1}=\varphi(h_1h_2)$. (by associativity)

thus $\varphi\in\mathrm{Hom}(G_m,G_{m'})$.

since the conjugation. $\mathrm{Im}\,\varphi=G_{m'}$. surjective.

let $\varphi(h_1)=\varphi(h_2)$, $g_0h_1g_0^{-1}=g_0h_2g_0^{-1}$. by cancelation law in subgroup $G_{m'}$, $h_1=h_2$.

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

$\begin{pmatrix} \bar{1} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} \\ \bar{2} \end{pmatrix}$ in same orbit $\quad$ it's corrsponding $|Gm_1| = \frac{|G|}{|Orbm_1|} = 2$.

$Orbm_1 = \left\{ \begin{pmatrix} \bar{1} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{0} \\ \bar{2} \end{pmatrix} \right\}$

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

2) $gm_2 = m_2 = \begin{pmatrix} \bar{0} \\ \bar{0} \end{pmatrix}$ for any $g \in G$. $\quad$ it's corrsponding $Gm_2 = G$.

$Orbm_2 = \left\{ \begin{pmatrix} \bar{0} \\ \bar{0} \end{pmatrix} \right\}$ $\quad Gm_2 = G$.

3) $\begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}\begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{2} \\ \bar{2} \end{pmatrix}, \begin{pmatrix} \bar{2} & 0 \\ 0 & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{2} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{2} & \bar{0} \end{pmatrix}\begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} \\ \bar{2} \end{pmatrix}$ $|Orbm_3| = 4$, it's corresponding $|Gm_3| = \frac{|G|}{|Orbm_3|} = 2$

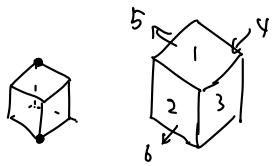
$Orbm_3 = \left\{ \begin{pmatrix} \bar{1} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{2} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{2} \end{pmatrix}, \begin{pmatrix} \bar{2} \\ \bar{1} \end{pmatrix} \right\}$.

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

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

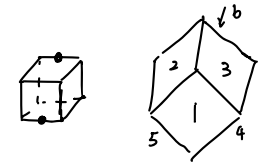
Hint. The group of the rotational symmetries of a cube consists of the following 24 elements: the identity, the rotations through 120° and 240° about 4 axes connecting the opposite vertices of the cube, the rotations through 180° about 6 axes connecting the midpoints of the opposite edges, and the rotations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

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

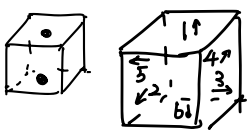
1) 

120° $\quad$ 2 cycle $\quad$ $1 \to 5 \to 4 \to 1$ $\quad$ $2 \to 3 \to 6 \to 2$ $\quad$ $|M^g| = 3^2$ $\quad$ 4 axes

240° $\quad$ 2 cycle $\quad$ $1 \to 4 \to 5 \to 1$ $\quad$ $2 \to 6 \to 3 \to 2$ $\quad$ $|M^g| = 3^2$ $\quad$ 4 axes

2) 

180° $\quad$ 3 cycle $\quad$ $1 \rightleftarrows 6$ $\quad$ $2 \rightleftarrows 3$ $\quad$ $4 \rightleftarrows 5$ $\quad$ $|M^g| = 3^3$ $\quad$ 6 axes

3) 

90°, 270° $\quad$ 3 cycle $\quad$ (1), (6) $\quad$ 90°: $5 \to 2 \to 3 \to 4 \to 5$ $\quad$ $|M^g| = 3^3 \times 2$ $\quad$ 3 axes

270°: $5 \to 4 \to 3 \to 2 \to 5$

180° $\quad$ 4 cycle $\quad$ (1) (6) $\quad$ $2 \rightleftarrows 4$ $\quad$ $3 \rightleftarrows 5$ $\quad$ $|M^g| = 3^4$ $\quad$ 3 axes

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

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

HW5. Week 14th.

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.*

Pf: $a^2 + (-b^2) = a^2 + (-b^2) + a\cdot b - b\cdot a$ (commutivity of $\cdot$)

$= (a^2 + a\cdot b) + [(-b)\cdot b + (-b)\cdot a]$ (commutivity, associativity of $+$; lemma 15.1.2)

$= a(a+b) + (-b)(b+a)$ (left distributivity)

$= [a + (-b)](a+b)$ (commutivity of $+$, right distributivity)

$= (a+b)(a+(-b))$ (commutivity of $\cdot$)

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

Hint. Show that if $x \neq \mathbf{0}$ then $x^n = \mathbf{1}$ 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. $\exists x \in R.$ 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 $x^{|i-j|} = 1$ 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*
- char $F = 3$

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

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

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

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

RHS$= (a_1,b_1)\cdot(a_2,b_2) + (a_1,b_1)\cdot(a_3,b_3) = (a_1a_2 - b_1b_2,\ a_1b_2 + a_2b_1) + (a_1a_3 - b_1b_3,\ a_1b_3 + b_1a_3)$.

$= (a_1a_2 + a_1a_3 - b_1b_2 - b_1b_3,\ a_1b_2 + a_1b_3 + b_1a_2 + b_1a_3) =$ LHS.

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

RHS$= (a_1,b_1)\cdot(a_3,b_3) + (a_2b_2)\cdot(a_3,b_3) = (a_1a_3 - b_1b_3,\ a_1b_3 + b_1a_3) + (a_2a_3 - b_2b_3,\ a_2b_3 + a_3b_2)$

$= (a_1a_3 + a_2a_3 - b_1b_3 - b_2b_3,\ a_1b_3 + a_2b_3 + b_1a_3 + b_2a_3) =$ LHS.

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

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

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

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 $\Phi\colon F \to \mathbb{C}$,*

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

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

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

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

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

V. distributivity is shown by distributivity of matrix operation.
$A(B+C) = AB + AC$ $(A+B)C = AC + BC$ for any matrix.

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

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

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

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

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

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

$$\Phi(A_1 A_2) = \Phi\begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -a_2b_1 - a_1b_2 & -b_1b_2 + a_1a_2 \end{pmatrix} = (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i = (a_1 + b_1 i)(a_2 + b_2 i) = \Phi(A_1) \cdot \Phi(A_2)$$

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. $\exists\ \Phi: \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{3}]$

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).

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

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

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

$$I+J=\{a+b \mid a\in I, b\in J\}, \quad IJ=\{a_1b_1+\cdots a_nb_n \mid a_1,\dots,a_n\in I, b_1,\dots,b_n\in J\}.$$

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). $I+J$. $\forall\ a_1+b_1,\ a_2+b_2 \in I+J$. $r\in R$.

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

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

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

① denote $N=\max(N_1, N_2)$ since $0\in I$. denote $a_j^2 \cdot a_i^1 = 0$ where $N_1+1\le i\le N$ $N_2+1\le j\le N$.

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

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

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

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

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

thus we have $I(J+J') \subset IJ+IJ'$

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

iii) $I=(a_1,\dots,a_n)=\{r_1a_1+r_2a_2+\cdots+r_na_n \mid r_i\in R,\ i\in[1:n]\}$

$J=(b_1,\dots,b_m)=\{p_1b_1+p_2b_2+\cdots+p_mb_m \mid p_j\in R,\ j\in[1:m]\}$.

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

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

thus $IJ=(a_ib_j,\ i\in[1:n],\ j\in[1:m])$.

Exercise 16.2. *Let ξ 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.

Pf: $\xi^3 = 1$.

$\xi = e^{\frac{2\pi k i}{3}}$ → i) $\xi = 1$ $a+b \in \mathbb{Z}$.

$a+b$ have inverse iff $a+b = \pm 1$.

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

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

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 $f \mid 1+\sqrt{3}$. $\exists\, h_1, h_2 \in R$. $2 = f h_1$ $1+\sqrt{-3} = f h_2$.

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

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

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

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

thus $N(f) = 1$ $N(h_1) = N(h_2) = 4$ or $N(f) = 4$ $N(h_1) = N(h_2) = 1$.

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

① $h_1 = \pm 1$. no $h_2 \in R$. s.t. $1+\sqrt{3} = \pm 2 \cdot h_2$. ② $h_2 = \pm 1$. no $h_1 \in R$ 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 $\bar{a}\cdot(\bar{b}+\bar{c}) = \bar{a}\cdot\bar{b} + \bar{a}\cdot\bar{c}$

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

②⑤ by def of multiplication. ①④ by def. of addition of quotient group.

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. $f = hg$.

thus $\bar{f} = \overline{hg} = \bar{h}\cdot\bar{g}$. 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.

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

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

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

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

which implies φ preserves the addition. for multiplication, similarly.

by def. φ is surjective.

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

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

thus $t - \frac{-b-i\sqrt{4ac-b^2}}{2a} \mid h$ and $t - \frac{-b+i\sqrt{4ac-b^2}}{2a} \mid h$ thus $at^2+bt+c \mid h \Rightarrow \bar{g_1} = \bar{g_2}$.

whence φ 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: $\varphi: R/I \to \mathbb{Z}/5\mathbb{Z}$ $\quad \varphi(\overline{a+bi}) = \overline{2a+b}$

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

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

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

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

if $\varphi(\overline{a_1+b_1 i}) = \varphi(\overline{a_2+b_2 i})$. then $\overline{(a_1-a_2)+(b_1-b_2)i} = \bar{0}$ 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. $(2+i) \mid (a_1-a_2)+(b_1-b_2)i$.

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

φ 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).

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

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

$$
\begin{array}{r|l}
 & t^3 - t^2 + \bar{1} \\
\hline
t^2+t+\bar{1} & t^5 + \bar{2}t + \bar{1} \\
 & t^5 + t^4 + t^3 \\
\hline
 & -t^4 - t^3 + \bar{2}t + \bar{1} \\
 & -t^4 - t^3 - t^2 \\
\hline
 & t^2 + \bar{2}t + \bar{1} \\
 & t^2 + t + \bar{1} \\
\hline
 & t
\end{array}
$$

thus. we have $f = g_1(t^3 - t^2 + \bar{1}) + t$. i.e. $g_1 \nmid f$

similarly. $f = g_2(t^3 - t^2 - t) + t + \bar{1}$ i.e. $g_2 \nmid f$

$f = g_3(t^3 - 2t^2 + t) + t + \bar{1}$ i.e. $g_3 \nmid f$

thus. there is no g s.t. $g \mid f$.

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. $g \in k[t]$ and $\deg g \le 4$.

1) suppose $f = (t^4 + a_3t^3 + a_2t^2 + a_1t + a_0)(t^4 + b_3t^3 + b_2t^2 + b_1t + b_0)$.

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

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

$a_2 + b_2 = \bar{1}$. 1). $\begin{cases} a_2 = \bar{1} \\ b_2 = \bar{0} \end{cases} \Rightarrow a_3 + b_3 = \bar{0} \Rightarrow$ 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^5 in f. ii) impossible. in that case t^7 could not appear in f.

or 2) $\begin{cases} a_2 = \bar{0} \\ b_2 = \bar{1} \end{cases} \Rightarrow a_3 + b_3 + \bar{1} = \bar{0} \Rightarrow$ 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. $f = (t^3 + a_2t^2 + a_1t + a_0)(t^5 + b_4t^4 + b_3t^3 + b_2t^2 + b_1t + b_0)$.

$f = t^8 + (a_2+b_4)t^7 + (b_3 + a_2b_4 + a_1)t^6 + (b_2 + a_2b_3 + a_1b_4 + a_0)t^5 + (b_1 + a_2b_2 + a_1b_3 + a_0b_4)t^4$

$+ (b_0 + a_2b_1 + a_1b_2 + a_0b_3)t^3 + (a_2b_0 + a_1b_1 + a_0b_2)t^2 + (a_0b_1 + a_1b_0)t + a_0b_0$.

$\begin{cases} a_0 = b_0 = \bar{1} \\ a_2 + b_4 = \bar{1} \\ b_3 + a_1 = \bar{0} \\ a_1 + b_1 = \bar{1} \\ a_2 + b_2 = \bar{1} \end{cases}$

i) let $a_1 = \bar{0}$. $\Rightarrow b_1 = \bar{1}$, $b_3 = \bar{0}$, $a_2 = \bar{1}$, $b_2 = \bar{0}$

and by coe. of t^4: $b_1 + a_2b_3 + a_1b_3 + a_0b_4 = \bar{0}$. $\Rightarrow \bar{1} + \bar{0} + \bar{0} + b_4 = \bar{0}$ $\Rightarrow b_4 = \bar{1}$.

but by coe. of t^7: $a_2 + b_4 = \bar{1}$ $\Rightarrow b_4 = \bar{0}$ contradicts.

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.

$\Rightarrow b_1 = \bar{0}$, $b_3 = \bar{1}$, $b_2 = \bar{0}$, $a_2 = \bar{1}$

thus a_1 not exist. thus case (2) is impossible.

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

$$
\begin{array}{r|l}
t^2+t+1 & t^6 - t^4 + t^3 - t + 2 \\
\hline
 & t^8 + t^7 + \qquad\qquad t^2 + t + 1 \\
 & t^8 + t^7 + t^6 \\
\hline
 & -t^6 \\
 & -t^6 - t^5 - t^4 \\
\hline
 & t^5 + t^4 \\
 & t^5 + t^4 + t^3 \\
\hline
 & -t^3 + t^2 + t \\
 & -t^3 - t^2 - t \\
\hline
 & 2t^2 + 2t + 1 \\
 & 2t^2 + 2t + 2 \\
\hline
 & -1
\end{array}
$$

since $-1 = \bar{1} \neq \bar{0}$

thus. $g \nmid f$.

(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 $(\mathbb{Z}/2\mathbb{Z})[t]$, $\varphi = \sum_{j=0}^{n} a_j t^j \mapsto \overline{\varphi} = \sum_{j=0}^{n} \overline{a}_j t^j$.
Clearly $\overline{\varphi\psi} = \overline{\varphi}\overline{\psi}$. Notice that $\overline{f}$ is irreducible over $\mathbb{Z}/2\mathbb{Z}$.

Pf: consider mapping $\Phi : \mathbb{Z}[t] \to (\mathbb{Z}/2\mathbb{Z})[t]$ $\varphi = \sum_{j=0}^{n} a_j t^j \mapsto \overline{\varphi} = \sum_{j=0}^{n} \overline{a_j} t^j$

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

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

$\overline{f} = t^5 + t^2 + \bar{1}$. by Problem 18.3. $\overline{f}$ 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. chark 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 $\mathbb{Z}/2\mathbb{Z}[x]/(t^3+t^2+\bar{1})$ of order 8.

"x"

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

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

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

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

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

"+"

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

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

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 $a\bar{x}^2 + b\bar{x} + c \mid a, b, c \in \mathbb{Z}/3\mathbb{Z}$, find $(\bar{x}^3+\bar{1})^{-1}$.*

Hint. Follow the proof of Proposition 17.2.

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

$g \nmid f$. 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 $h_1 = \bar{2}$ $h_2 = x$. $\bar{2}(x^3+x+\bar{2}) + x(x^2+\bar{1}) = \bar{1}$.

in $\mathbb{Z}/3\mathbb{Z}[t]/f$. $\overline{h_2} \cdot \bar{g} = \overline{h_2 g} = \bar{1}$. $\bar{g}$ has inverse $\overline{h_2}$. i.e. $(\bar{x}^2+\bar{1})^{-1} = \bar{x}$.