

## MATH 601 HOMEWORK (DUE 9/11)

HIDENORI SHINOHARA

**Exercise.** (1) Show that  $2 \times 2$  matrices give a functor,  $M_2$ , from the category of rings to itself,  $R \mapsto M_2(R)$ .

*Proof.* Let  $R, R'$  be rings and  $\phi \in \text{Hom}(R, R')$ . Let  $M_2(\phi) : M_2(R) \rightarrow M_2(R')$  be defined such that

$$(M_2(\phi)) \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \begin{bmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{bmatrix}.$$

We claim that  $M_2$  is indeed a functor.

- Claim 1: For any  $\phi \in \text{Hom}(R, R')$ ,  $M_2(\phi) \in \text{Hom}(M_2(R), M_2(R'))$ . In other words, we want to show that  $M_2(\phi)$  is a ring homomorphism for any  $\phi$ .

$$\begin{aligned} (M_2(\phi)) \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) &= (M_2(\phi)) \left( \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \right) \\ &= \begin{bmatrix} \phi(a+e) & \phi(b+f) \\ \phi(c+g) & \phi(d+h) \end{bmatrix} \\ &= \begin{bmatrix} \phi(a) + \phi(e) & \phi(b) + \phi(f) \\ \phi(c) + \phi(g) & \phi(d) + \phi(h) \end{bmatrix} \\ &= \begin{bmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{bmatrix} + \begin{bmatrix} \phi(e) & \phi(f) \\ \phi(g) & \phi(h) \end{bmatrix} \\ &= (M_2(\phi)) \begin{bmatrix} a & b \\ c & d \end{bmatrix} + (M_2(\phi)) \begin{bmatrix} e & f \\ g & h \end{bmatrix} \end{aligned}$$

$$\begin{aligned}
& (M_2(\phi)) \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \\
&= (M_2(\phi)) \left( \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} \right) \\
&= \begin{bmatrix} \phi(ae + bg) & \phi(af + bh) \\ \phi(ce + dg) & \phi(cf + dh) \end{bmatrix} \\
&= \begin{bmatrix} \phi(a)\phi(e) + \phi(b)\phi(g) & \phi(a)\phi(f) + \phi(b)\phi(h) \\ \phi(c)\phi(e) + \phi(d)\phi(g) & \phi(c)\phi(f) + \phi(d)\phi(h) \end{bmatrix} \\
&= \begin{bmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{bmatrix} \begin{bmatrix} \phi(e) & \phi(f) \\ \phi(g) & \phi(h) \end{bmatrix} \\
&= (M_2(\phi)) \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) (M_2(\phi)) \left( \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right)
\end{aligned}$$

Therefore,  $M_2(\phi)$  is indeed a ring homomorphism.

- For any ring  $R$  and the identity function  $\text{Id}_R$ ,  $M_2(\text{Id}_R)$  is the identity map on  $M_2(R)$  because it maps each element in a given matrix to itself.
- Let  $f \in \text{Hom}(A, B)$ ,  $g \in \text{Hom}(B, C)$ .

$$\begin{aligned}
(M_2(f \circ g)) \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) &= \begin{bmatrix} (f \circ g)(a) & (f \circ g)(b) \\ (f \circ g)(c) & (f \circ g)(d) \end{bmatrix} \\
&= \begin{bmatrix} f(g(a)) & f(g(b)) \\ f(g(c)) & f(g(d)) \end{bmatrix} \\
&= M_2(f) \left( \begin{bmatrix} g(a) & g(b) \\ g(c) & g(d) \end{bmatrix} \right) \\
&= M_2(f) \left( M_2(g) \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) \right) \\
&= (M_2(f) \circ M_2(g)) \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right).
\end{aligned}$$

Therefore,  $M_2$  is indeed a functor. □

**Exercise.** (Problem 4 from More exercises)

- (1) If  $F$  is a functor from category  $C$  to a category  $C'$  and  $G$  is a functor from a category  $C'$  to a category  $C''$ , under what conditions is a composite functor,  $G \circ F : C \rightarrow C''$  defined?
- (2) For a ring  $R$  write  $GL_2(R)$  for the set of all invertible  $2 \times 2$  matrices with entries in  $R$ . List the exercises above and the sections of the handouts which combine to give a proof that  $GL_2$  is a functor from rings to groups.
- (3) For a commutative ring  $R$  let  $SL_2(R)$  denote the set of all  $2 \times 2$  matrices with entries in  $R$  and determinant 1. Is  $SL_2$  a functor from commutative rings to groups?
- (4) Let  $k$  be a field. There is a natural right action of  $GL_2(k)$  on  $\mathbb{P}^1(k)$ . Write down how an element of  $GL_2(k)$  acts on an element of  $\mathbb{P}^1(k)$  using homogeneous coordinates.
- (5) Determine the subgroup of  $GL_2(k)$  which acts as the identity on  $\mathbb{P}^1(k)$ .

*Proof.*

- (1) A composition of two functors is always a functor.
- (2) Exercise 1 from More exercises shows that  $M_2$  is a functor from the category of rings to itself. From “Units as a functor” in the handout from the first lecture, we know that passing from rings to units is a functor from the category of rings to the category of groups. Then by composing  $M_2$  with the operation to take units, we get  $GL_2$ . Exercise 4(a) from More exercises shows that a composition of two functors is a functor. Thus  $GL_2$  is a functor.
- (3) Yes, it is.
- (4)

$$(x_0 : x_1) \star \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (ax_0 + cx_1 : bx_0 + dx_1).$$

- (5) We claim that the subgroup  $\{tI \mid t \in k^\times\}$  acts as the identity on  $\mathbb{P}^1(k)$ .  $(x_0 : x_1) \star tI = (tx_0 : tx_1) = (x_0 : x_1)$ . Let  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{P}^1(k)$ . Suppose  $A$  acts as the identity on  $\mathbb{P}^1(k)$ .

- Case 1:  $b \neq 0$ . Then  $(1 : 0) \star \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (a : b)$ . Since  $b \neq 0$ ,  $(t \cdot 1, t \cdot 0) \neq (a, b)$  for any  $t \in k^\times$ . Therefore,  $A$  does not act as the identity on  $\mathbb{P}^1(k)$ .
- Case 2:  $d \neq 0$ . Then  $(0 : 1) \star \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (c : d)$ . Since  $d \neq 0$ ,  $(t \cdot 0, t \cdot 1) \neq (c, d)$  for any  $t \in k^\times$ . Therefore,  $A$  does not act as the identity on  $\mathbb{P}^1(k)$ .
- Case 3:  $b = d = 0$  and  $a \neq d$ . Then  $(1 : 1) \star \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (a : d)$ . Since  $a \neq d$ ,  $(t \cdot 1, t \cdot 1) \neq (a, d)$  for any  $t \in k^\times$ . Therefore,  $A$  does not act as the identity on  $\mathbb{P}^1(k)$ .

This means that  $b = d = 0$  and  $a = d$ . Since  $A$  is invertible,  $a \neq 0$ . Thus  $A$  is indeed an element of  $\{tI \mid t \in k^\times\}$ . Therefore,  $\{tI \mid t \in k^\times\}$  is exactly the set of elements that act as the identity on  $\mathbb{P}^1(k)$ . □

**Exercise.** (Problem 5 from More exercises)

- (1) Compute  $|SL_2(\mathbb{Z}/p)|$ , the number of elements in  $SL_2(\mathbb{Z}/p)$ , when  $p$  is an odd prime number.
- (2) Find all conjugacy classes of  $SL_2(\mathbb{Z}/3)$ . For each conjugacy class,  $C$ , compute  $|C|$  and  $|Z_C|$ . Present your results in the form of a table.

*Proof.*

- (1) From the previous homework, we know that  $|GL_2(\mathbb{Z}/p)| = p^4 - p^3 - p^2 + p$ . We claim that  $|SL_2(\mathbb{Z}/p)| = (p^4 - p^3 - p^2 + p)/(p - 1)$ . For each  $i = 1, 2, \dots, p - 1$ , let  $S_i$  denote the set of all matrices in  $GL_2(\mathbb{Z}/p)$  whose determinant is  $i$ . Then  $GL_2(\mathbb{Z}/p) = \bigcup S_i$  and  $S_i$ 's are disjoint. Let  $i \neq j \in \{1, \dots, p - 1\}$ . Let  $f : S_i \rightarrow S_j$  be the function that multiplies the first row of a matrix by  $j/i$ .  $f$  is well-defined because multiplying the first row of a matrix by  $j/i$  multiplies the determinant by  $j/i$ .  $f$  is injective since  $g \circ f$  is the identity map on  $S_i$  where  $g : S_j \rightarrow S_i$  is the map that multiplies the first row of a matrix by  $i/j$ .

This implies that  $|S_i| \leq |S_j|$  for each  $i \neq j$ . This is only possible if  $|S_i| = |S_j|$  for each  $i \neq j$ . Therefore,  $|S_i| = |GL_2(\mathbb{Z}/p)|/(p-1) = p^3 - p$ .

(2) The following table is generated by the attached Python code.

$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}$
$\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix}$
$\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$

(3) Every nonzero vector is a eigenvector for some matrix in each conjugacy class. In the following table, each column lists a matrix from each conjugacy class for which the vector is an eigenvector. (Each row corresponds to a conjugacy class above in the same order.)

$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 2 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 1 \\ 2 \end{bmatrix}$	$\begin{bmatrix} 2 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 2 \\ 1 \end{bmatrix}$	$\begin{bmatrix} 2 \\ 2 \end{bmatrix}$
$\begin{bmatrix} 2 & 0 \\ 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 2 \end{bmatrix}$
$\begin{bmatrix} 2 & 0 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 2 & 2 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 2 \\ 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$
$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$

□

**Exercise.** (Problem 8 from More exercises) Consider the subgroup,  $D_5 = \langle (12345), (14)(23) \rangle \subset S_5$ .

(1) Set  $a = (12345)$  and compute  $a^{-1}$ .

- (2) Set  $b = (14)(23)$  and compute  $aba^{-1}$ .
- (3) Show that every element in  $D_5$  may be written in the form  $a^i b^j$  for some  $i, j \in \mathbb{Z}$ .
- (4) Compute  $|D_5|$ .
- (5) Draw a regular pentagon with vertices labeled successively 1, 2, 3, 4, 5. Show that  $D_5$  acts on the pentagon by describing the action in geometric terms.
- (6) Recall that a group acts on its subgroups by conjugation,  $H \subset G, H \mapsto gHg^{-1}$ . The orbits of this action are called conjugacy classes of subgroups. Determine all the conjugacy classes of subgroups of  $D_5$ .

*Proof.*

- (1)  $a$  sends 1 to 2, 2 to 3,  $\dots$ . We want  $a^{-1}$  to do the opposite. Thus  $a^{-1} = (15432)$ . Since  $(12345)(15432) = (15432)(12345) = (1)$ ,  $(15432)$  is indeed  $a^{-1}$ .
- (2)  $aba^{-1} = (a(1)a(4))(a(2)a(3)) = (25)(34)$ .
- (3)  $ba = (14)(23)(12345) = (13)(45)$ , and  $a^{-1}b = (15432)(14)(23) = (13)(45)$ . Therefore,  $ba = a^{-1}b$ . We claim that  $ba^n = a^{-n}b$  for every  $n \in \mathbb{N}$ . Suppose  $ba^n = a^{-n}b$  for some  $n \in \mathbb{N}$ . Then  $ba^{n+1} = (ba^n)a = (a^{-n}b)a = a^{-n}(ba) = a^{-n}a^{-1}b = a^{-(n+1)}b$ . By mathematical induction,  $ba^n = a^{-n}b$  for every  $n \in \mathbb{N}$ .

For any  $n \in \mathbb{N}$ ,  $ba^n = a^{-n}b$ , so  $a^n ba^n = b$ , and thus  $a^n b = ba^{-n}$ . Therefore, we have  $ba^k = a^{-k}b$  for every  $k \in \mathbb{Z}$ .

We claim that for any  $i, j \in \mathbb{Z}$ ,  $b^j a^i$  can be written in the desired form. Since  $b^2 = e$ , we consider two cases based on the parity of  $j$ . If  $j$  is even, then  $b^j = e$ , so  $b^j a^i = a^i$ . If  $j$  is odd, then  $b^j = b$ , so  $b^j a^i = ba^i = a^{-i}b$  as shown above.

We will prove the general case. By the argument above, it suffices to show that every element in  $D_5$  can be represented as a word of length  $\leq 2$ . Let  $x_1^{i_1} \cdots x_k^{i_k} \in D_5$  be given where  $i_1, \dots, i_k \in \mathbb{Z}$  and each  $x_i$  is either  $a$  or  $b$ . Since  $D_5$  is generated by  $a, b$ , every element can be represented in this form. We will show that every element in  $D_5$  can be represented as a word of length  $\leq 2$  by using strong induction. If  $k \leq 2$ , then we are done. Suppose that we can represent every element in  $D_5$  of length  $\leq k$  as a word of length  $\leq 2$  for some  $k \geq 2$ . Let  $x = x_1^{i_1} \cdots x_{k+1}^{i_{k+1}} \in D_5$ . If  $x_1 = x_2$ , then  $x = x_2^{i_1+i_2} x_3^{i_3} \cdots x_{k+1}^{i_{k+1}}$ , so by the inductive hypothesis, this can be represented as a word of length  $\leq 2$ . If  $x_2 = x_3$ , then  $x = x_1^{i_1} x_2^{i_2+i_3} x_4^{i_4} \cdots x_{k+1}^{i_{k+1}}$ , so by the inductive hypothesis, this can be represented as a word of length  $\leq 2$ . Suppose  $x_1 \neq x_2$  and  $x_2 \neq x_3$ . Then there are two cases:

- Case 1:  $(x_1, x_2, x_3) = (a, b, a)$ . By the argument above,  $b^{i_2} a^{i_3}$  can be represented as  $a^i b^j$  for some  $i, j \in \mathbb{Z}$ . Therefore,  $a^{i_1} (b^{i_2} a^{i_3}) = a^{i_1} (a^i b^j) = a^{i_1+i} b^j$ , so  $x$  can be represented as a word of length  $k$ . By the inductive hypothesis,  $x$  can be represented as a word of length  $\leq 2$ .
  - Case 2:  $(x_1, x_2, x_3) = (b, a, b)$ . By the argument above,  $b^{i_1} a^{i_2}$  can be represented as  $a^i b^j$  for some  $i, j \in \mathbb{Z}$ . Therefore,  $(b^{i_1} a^{i_2}) b^{i_3} = (a^i b^j) b^{i_3} = a^i b^{j+i_3}$ . By the inductive hypothesis,  $x$  can be represented as a word of length  $\leq 2$ .
- (4)
    - $a^1 = a \neq (1)$ .
    - $a^2 = (13524) \neq (1)$ .
    - $a^3 = (14253) \neq (1)$ .
    - $a^4 = (15432) \neq (1)$ .
    - $a^5 = (1)$ .

Therefore, the order of  $a$  is 5. Since  $b \neq (1)$  and  $b^2 = (1)$ , the order of  $b$  is 2. We claim that there are exactly 10 elements in  $D_5$ .

- Claim 1:  $|D_5| \leq 10$ . Let  $x \in D_5$ . Then there exist  $i, j \in \mathbb{Z}$  such that  $x = a^i b^j$ . Since the order of  $a$  is 5 and the order of  $b$  is 2, we can assume that  $0 \leq i \leq 4$  and  $0 \leq j \leq 1$ . Therefore,  $D_5 \subset \{a^i b^j \mid 0 \leq i \leq 4, 0 \leq j \leq 1\}$ . Thus there are at most 10 elements in  $D_5$ .
- Claim 2:  $|D_5| \leq 10$ . Let  $a^i b^j, a^{i'} b^{j'} \in \{a^i b^j \mid 0 \leq i \leq 4, 0 \leq j \leq 1\}$ . Suppose  $a^i b^j = a^{i'} b^{j'}$ . Then  $a^{i-i'} = b^{j'-j}$ . We have calculated all the powers of  $a$  above, and none of them is equal to  $b$ . Therefore,  $i - i' \equiv 0 \pmod{5}$  and  $j - j' \equiv 0 \pmod{2}$ . Since  $0 \leq i, i' \leq 4, 0 \leq j, j' \leq 1$ ,  $i = i'$  and  $j = j'$ . This implies that the set  $\{a^i b^j \mid 0 \leq i \leq 4, 0 \leq j \leq 1\}$  contains exactly 10 elements. Since the set is a subset of  $D_5$ ,  $D_5$  contains at least 10 elements.

Therefore,  $D_5$  contains exactly 10 elements.

- (5)  $a$  corresponds to a reflection, and  $b$  corresponds to a rotation as in the figure.
- (6) We will first identify all the subgroups of  $D_5$ . By Lagrange's Theorem, a subgroup must have exactly 1, 2, 5, or 10 elements. Since the case when the order is 1 or 10 is trivial, we will consider order 2 and 5.

- Subgroups of order 2. They are cyclic groups generated by elements of order 2.  $a$  has order 5, so  $a$  does not form a subgroup of order 2. The order of  $a^2, a^3, a^4$  must divide  $a^5$  by Lagrange's theorem since  $\langle a^i \rangle$  is a subset of  $\langle a \rangle$ . Since 5 is prime, the order of  $a^2, a^3, a^4$  must be 5. Thus none of  $a, a^2, a^3, a^4$  generate a subgroup of order 2. Moreover,  $a^5 = e$  does not form a subgroup of order 2.

The remaining elements are  $b, ab, a^2b, a^3b, a^4b$ .

- $b = (14)(23)$ , and  $b^2 = (1)$ .
- $ab = (12345)(14)(23) = (15)(24)$ , and  $(ab)^2 = (1)$ .
- $a^2b = (12345)(15)(24) = (25)(34)$ , and  $(a^2b)^2 = (1)$ .
- $a^3b = (12345)(25)(34) = (12)(35)$ , and  $(a^3b)^2 = (1)$ .
- $a^4b = (12345)(12)(35) = (13)(45)$ , and  $(a^4b)^2 = (1)$ .

Thus  $\langle b \rangle, \langle ab \rangle, \langle a^2b \rangle, \langle a^3b \rangle, \langle a^4b \rangle$  are all the distinct subgroups of order 2.

- Subgroups of order 5. Since 5 is prime, they are cyclic groups generated by elements of order 5. As shown above, the only elements of order 5 are  $a, a^2, a^3, a^4$ , and they all generate the same subgroup. Thus  $\langle a \rangle$  is the only subgroup of order 5.

Now, we will determine all the conjugacy classes of subgroups of  $D_5$ . Since  $|H| = |gHg^{-1}|$  for each subgroup  $H$  and  $g \in G$ , it suffices to compare subgroups of the same order.

- Subgroups of order 1. The only subgroup of order 1 is the trivial group, and it is the only subgroup in its conjugacy class.
- Subgroups of order 2. The set of all the subgroups of order 2 are  $\{\langle a^i b \rangle \mid 0 \leq i \leq 4\}$ . Let  $0 \leq i \leq 4$  be given. Then  $a^3(a^i b)a^{-3} = a^{i+3}(ba^{-3}) = a^{i+3}a^3b = a^{i+6}b = a^{i+1}b$ . Therefore,  $\langle a^i b \rangle \sim \langle a^{i+1}b \rangle$  for each  $0 \leq i \leq 4$ . In other words, the set of all the subgroups of order 2 is an equivalence class.
- Subgroups of order 5. The only subgroup of order 5 is  $\langle a \rangle$ , and it is the only subgroup in its conjugacy class.

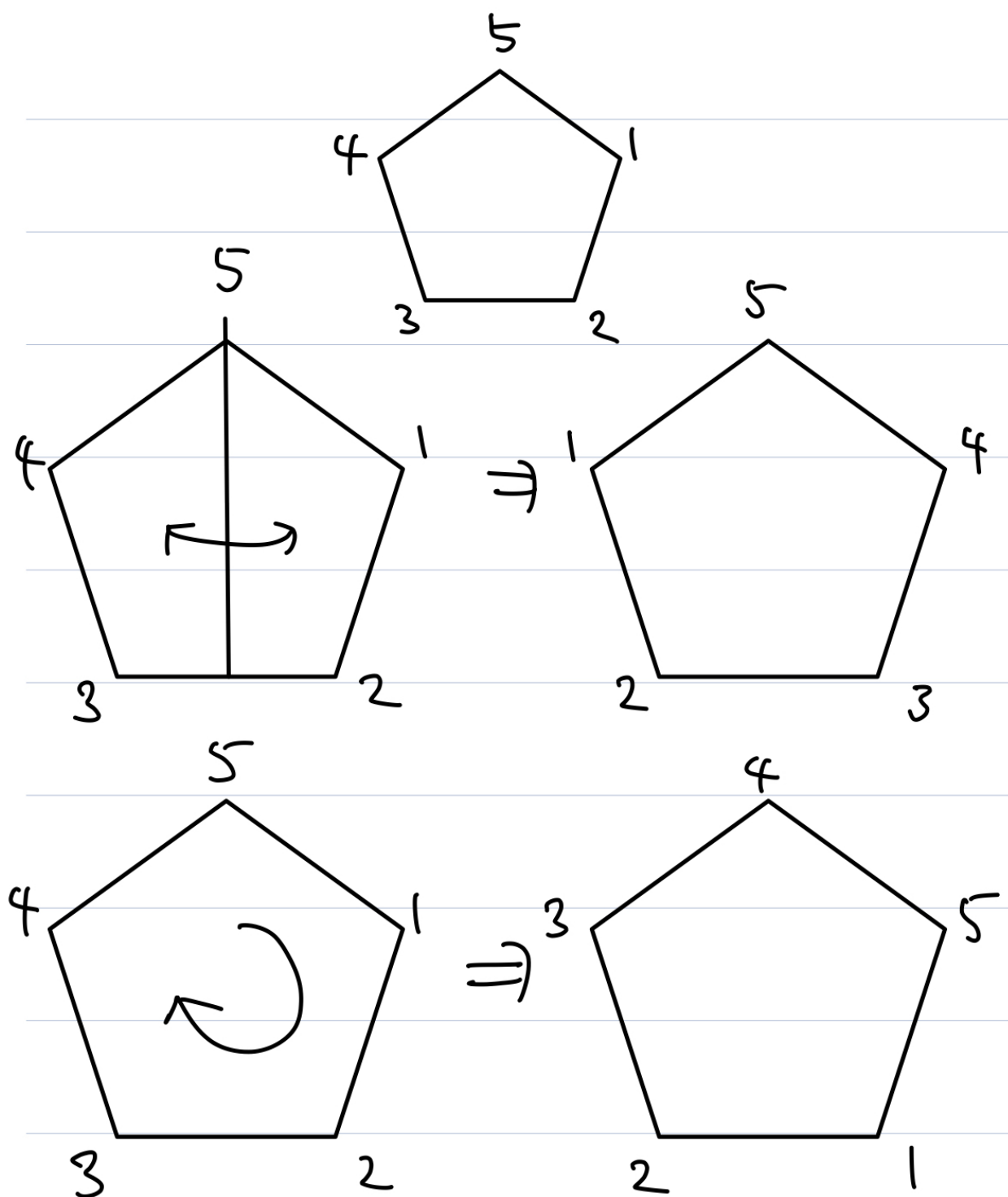


FIGURE 1. Interpret  $D_5$  geometrically

- Subgroups of order 10. The only subgroup of order 10 is itself, and it is the only subgroup in its conjugacy class.

Therefore, there are 4 conjugacy classes,  $\{\langle e \rangle\}, \{\langle a^i b \rangle \mid 0 \leq i \leq 4\}, \{\langle a \rangle\}, \{D_5\}$ .

□

**Exercise.** (Problem 9 from More exercises) Consider the subgroup  $B = \langle (12345), (1243) \rangle \subset S_5$ .

- Determine the number of elements in  $B$ .
- Show that  $B$  is a solvable group.

*Proof.* Let  $a = (12345), b = (1243)$ .

- Since the order of  $a$  is 5,  $5 \mid |B|$  by Lagrange's Theorem. Similarly,  $4 \mid |B|$  since  $|b| = 4$ . This implies that the order of  $B$  is at least 20. Let  $S = \{a^i b^j \mid 0 \leq i \leq 4, 0 \leq j \leq 3\}$ . We claim that  $B = S$ .

–  $S \subset B$ . This is trivial.

–  $B \subset S$ ?  $a^2 b = (1452) = ba$ , so  $ba^n = (ba)a^{n-1} = a^2(ba^{n-1}) = \dots = a^{2n}b \in S$  for each  $n \in \mathbb{N}$ . This is similar to Problem 8(iii) and can be shown more rigorously using mathematical induction. Since the order of  $a$  is finite,  $\forall n \in \mathbb{N}, a^{-n}$  can be expressed as a positive power of  $a$ . Therefore,  $ba^k \in S$  for each  $k \in \mathbb{Z}$ .

For any  $n \in \mathbb{N}, k \in \mathbb{Z}$ ,  $b^n a^k = b^{n-1}(ba^k) = b^{n-1}(a^{2k}b) = b^{n-2}(ba^{2k})b = \dots = a^{2nk}b^n \in S$ . This again can be shown more rigorously using mathematical induction. Since the order of  $b$  is finite,  $\forall n \in \mathbb{N}, b^{-n}$  can be expressed as a positive power of  $b$ . Therefore,  $b^k a^l \in S$  for each  $k, l \in \mathbb{Z}$ .

Using the same argument as Problem 8(iii), we can conclude that every element in  $B$  can be expressed as  $a^i b^j$ .

Therefore,  $B = S$ . Since we know that  $B$  contains at least 20 elements,  $S$  is exactly the set of elements in  $B$ . Thus  $|B| = 20$ .

- Let  $C = \{a^i b^j \mid i \in \{0, 1, 2, 3, 4\}, j \in \{0, 2\}\}$ . We claim that  $C$  is a subgroup of  $B$ . Let  $a^i b^j \in C$ . Then  $j = 0$  or  $2$ . Thus  $-j = j \pmod{4}$ .  $(a^i b^j)^{-1} = b^{-j} a^{-i} = b^j a^{-i} = a^{-2j} b^j \in C$ . Thus  $C$  is closed under multiplication. Since  $C$  contains the identity,  $C$  is nonempty. Any nonempty subset of a finite group that is closed under multiplication is a subgroup, so  $C$  is a subgroup.  $C$  contains 10 elements. Thus  $C$  is a normal subgroup of  $B$  because the index  $[B : C]$  is 2.

Since  $B/C$  is a group with 2 elements, it is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ , thus it is abelian.

Similarly,  $\langle a \rangle$  is a subgroup of  $C$  and the index  $[C : \langle a \rangle]$  is 2, so  $\langle a \rangle$  is a normal subgroup of  $C$ . Again,  $C/\langle a \rangle$  is a group with 2 elements, so it is abelian. Finally,  $\{e\}$  is a normal subgroup of  $\langle a \rangle$ . Since  $\langle a \rangle$  is abelian,  $\langle a \rangle/\{e\}$  is abelian.

Thus  $\{e\} \subset \langle a \rangle \subset C \subset B$  is a filtration by subgroups, so  $B$  is solvable.

□

**Exercise.** (Exercise 10 from More exercises) Let  $k$  be a field. The smallest subgroup of **Bijections** $(k^n, k^n)$  which contains  $GL_n(k)$  and the group of translations by elements of  $k^n$  is called the group of affine transformations of  $k^n$  and will be denoted  $Aff_n(k)$ .

- Let  $G = \left\{ \begin{bmatrix} * & v \\ 0 & 1 \end{bmatrix} \in GL_{n+1}(k) : * \in GL_n(k), v \in k^n \right\}$ . Here  $v$  is a column vector of length  $n$  and  $0$  is the row vector of length  $n$  in which all entries are 0. Finally  $1$  is the number 1. Show that  $G$  acts on column vectors in  $k^{n+1}$  whose last entry is 1.



- Describe a group isomorphism,  $h : G \rightarrow \text{Aff}_n(k)$ .
- Compute the order of  $G$  when  $k = \mathbb{Z}/p$  and  $n = 1$ .

*Proof.*

- Let  $w \in k^v$  be given. Then

$$\begin{bmatrix} * & v \\ 0 & 1 \end{bmatrix} \begin{bmatrix} w \\ 1 \end{bmatrix} = \begin{bmatrix} w' \\ 1 \end{bmatrix}$$

for some  $w' \in k^v$ ,  $k^v$  is closed under this action. The associativity of this action is guaranteed from linear algebra. The identity map maps any column vector to itself. Thus this is indeed a group action.

- Let  $M \in G$  be given. Let  $h(M)$  denote the function  $k^n \rightarrow k^n$  such that

$$v \mapsto \left[ \begin{array}{c|c} I_{n,n} & 0 \end{array} \right] M \begin{bmatrix} v \\ 1 \end{bmatrix}$$

- Group homomorphism?
- Injective?
- Surjective?

- When  $n = 1$ , there are exactly  $(p - 1)$   $1 \times 1$  matrices in  $GL_n(k)$ . Also, there are exactly  $(p - 1)$  vectors in  $k^n$ . Thus there are  $(p - 1)^2$  elements in  $G$ .

□