

# MATH 601 HOMEWORK (DUE 9/4)

HIDENORI SHINOHARA

**Exercise.** (2.1) Show that the function  $g : \mathbb{R} \rightarrow S^1$ ,  $g(r) = \exp(2\pi ir)$ , where  $i^2 = -1$ , satisfies the property that  $g(r) = g(r')$  if and only if  $r \sim r'$ . Use this to explicitly construct a bijective map from the orbit space of the action to  $S^1$ ,  $g : \mathbb{R}/\sim = \mathbb{Z}\backslash\mathbb{R} \rightarrow S^1$ .

*Proof.*

- Let  $r, r' \in \mathbb{R}$  such that  $r \sim r'$ . Let  $k \in \mathbb{Z}$  such that  $k * r' = r$ . Therefore,  $k + r' = r$ .

$$\begin{aligned} g(r) &= \exp(2\pi ir) \\ &= \exp(2\pi i(k + r')) \\ &= \exp(2\pi ik + 2\pi ir') \\ &= \exp(2\pi ik) \exp(2\pi ir') \\ &= \exp(2\pi ir') \\ &= g(r'). \end{aligned}$$

- Let  $r, r' \in \mathbb{R}$  such that  $g(r) = g(r')$ .

$$\begin{aligned} \exp(2\pi ir) = \exp(2\pi ir') &\implies \exp(2\pi i(r - r')) = 1 \\ &\implies \cos(2\pi(r - r')) + i \sin(2\pi(r - r')) = 1 \\ &\implies \sin(2\pi(r - r')) = 0 \\ &\implies r - r' \in \mathbb{Z} \\ &\implies \exists k \in \mathbb{Z}, r = k * r' \\ &\implies r \sim r'. \end{aligned}$$

Let  $g : \mathbb{Z}\backslash\mathbb{R} \rightarrow S^1$  be defined such that  $g([r]) = g(r)$  for each  $[r] \in \mathbb{Z}\backslash\mathbb{R}$ .

- Well-defined? Let  $[r] = [r'] \in \mathbb{Z}\backslash\mathbb{R}$ . Then  $r \sim r'$ . We showed that  $g(r) = g(r')$  if  $r \sim r'$  earlier. Therefore,  $g$  is indeed well-defined.
- Injective? Let  $[r], [r'] \in \mathbb{Z}\backslash\mathbb{R}$ . Suppose  $g([r]) = g([r'])$ . Then  $g(r) = g(r')$ . We showed earlier that this implies  $r \sim r'$ . In other words,  $[r] = [r']$ . Therefore,  $g$  is injective.

- Surjective? Let  $z \in S^1$ . Express  $z$  as  $re^{i\theta}$  where  $r, \theta \in \mathbb{R}$ . Since  $|z| = 1$ , we can assume that  $r = 1$  without loss of generality. (If  $r = -1$ , then  $e^{i\pi} = -1$ , so  $\theta$  can be redefined as  $\theta + \pi$ .)  
Then  $[\theta/2\pi]$  is an element in  $\mathbb{Z}/\mathbb{R}$ , and  $g([\theta/2\pi]) = g(\theta/2\pi) = \exp(2\pi i \cdot \theta/2\pi) = \exp(i\theta) = z$ . Therefore,  $g$  is indeed surjective.

□

**Exercise. (2.2)** Let  $\star : G \times S \rightarrow S$  be a left action of  $G$ . Show that  $s \star g = g^{-1} \star s$  defines a right action of  $G$  on  $S$ .

*Proof.* Let  $s \in S, g, h \in G$  be given.

$$\begin{aligned}
 (s \star g) \star h &= h^{-1} \star (s \star g) \\
 &= h^{-1} \star (g^{-1} \star s) \\
 &= (h^{-1}g^{-1}) \star s \\
 &= (gh)^{-1} \star s \\
 &= s \star (gh).
 \end{aligned}$$

Let  $e \in G$  denote the identity element and let  $s \in S$  be given.

$$\begin{aligned}
 s \star e &= e^{-1} \star s \\
 &= e \star s \\
 &= s.
 \end{aligned}$$

Therefore,  $\star$  is indeed a right action of  $G$  on  $S$ .

□

**Exercise. (2.3)**

- (1) Let  $h, h' \in G$  lie in the same conjugacy class. Show that  $h$  and  $h'$  have the same order.
- (2) Give an example of a group and two elements of the same order which do not lie in the same conjugacy class.

*Proof.* (1) Since  $h$  and  $h'$  lie in the same conjugacy class, there must exist an element  $g \in G$  such that  $h = g \star h'$ . In other words,  $h = g \cdot h' \cdot g^{-1}$ . We will show that  $h^n = g \cdot (h')^n \cdot g^{-1}$  for all  $n \in \mathbb{N}$  using mathematical induction.

- When  $n = 1$ , the statement is true.

- Suppose  $h^n = g \cdot (h')^n \cdot g^{-1}$  for some  $n \in \mathbb{N}$ .

$$\begin{aligned} h^{n+1} &= h^n \cdot h \\ &= (g \cdot (h')^n \cdot g^{-1}) \cdot (g \cdot h' \cdot g^{-1}) \\ &= g \cdot (h')^n \cdot (g^{-1} \cdot g) \cdot h' \cdot g^{-1} \\ &= g \cdot (h')^n \cdot h' \cdot g^{-1} \\ &= g \cdot (h')^{n+1} \cdot g^{-1}. \end{aligned}$$

Therefore,  $h^n = g \cdot (h')^n \cdot g^{-1}$  for all  $n \in \mathbb{N}$ .

For any  $n \in \mathbb{N}$ , if  $h^n = e$ , then  $g \cdot (h')^n \cdot g^{-1} = e$ , so  $(h')^n = g^{-1}g = e$ . For any  $n \in \mathbb{N}$ , If  $(h')^n = e$ , then  $h^n = geg^{-1} = e$ . Therefore,  $\forall n \in \mathbb{N}, h^n = e \iff (h')^n = e$ .

This implies that if the order of one of  $h$  or  $h'$  is infinite, the other has to be infinite as well. On the other hand, if the order of one of  $h$  or  $h'$  is finite, the other has to be finite as well. Suppose that the orders of  $h$  and  $h'$  are finite and let  $n$  denote the order of  $h$ . Then  $h^n = e$  and  $h^m \neq e$  for each natural number  $m < n$ . Then  $(h')^n = e$  and  $(h')^m \neq e$  for each natural number  $m < n$ . Therefore, the order of  $h'$  is  $n$  as well.

We showed that, regardless of whether the order is finite,  $h$  and  $h'$  have the same order.

- (2) We will consider the Klein 4-group  $K = \{e, a, b, c\}$ . Since  $a^2 = b^2 = e$ ,  $a$  and  $b$  have the order 2. Suppose that  $a$  and  $b$  lie in the same conjugacy class. Then there must exist a  $g \in K$  such that  $a = gbg^{-1}$ . Since  $K$  is abelian,  $a = gbg^{-1} = gg^{-1}b = eb = b$ . This is a contradiction, so  $a$  and  $b$  do not lie in the same conjugacy class. Thus we found two elements of the same order which do not lie in the same conjugacy class.

□

**Exercise.** (2.4) Construct a bijection between  $\mathbb{P}_k^n$  and the set of all one-dimensional subspaces of the vector space,  $k^{n+1}$ .

*Proof.* Let  $F$  be the mapping from  $\mathbb{P}_k^n$  to the set of all one-dimensional subspaces of  $k^{n+1}$  defined by  $F(x_0 : \cdots : x_n) = \{(tx_0, \cdots, tx_n) \mid t \in k\}$ . We claim that this is a bijection.

- Well-defined? Let  $(x_0 : \cdots : x_n) = (y_0 : \cdots : y_n) \in \mathbb{P}_k^n$  be given. Then there must exist a  $t \in k^\times$  such that  $(x_0, \cdots, x_n) = (ty_0, \cdots, ty_n)$ .
  - For any  $(sx_0, \cdots, sx_n) \in F(x_0 : \cdots : x_n)$ ,  $(sx_0, \cdots, sx_n) = (sty_0, \cdots, sty_n) \in F(y_0 : \cdots : y_n)$ .

- For any  $(sy_0, \dots, sy_n) \in F(y_0 : \dots : y_n)$ ,  $(sy_0, \dots, sy_n) = ((s/t)ty_0, \dots, (s/t)ty_n) = ((s/t)x_0, \dots, (s/t)x_n) \in F(x_0 : \dots : x_n)$ .

Therefore,  $F(x_0 : \dots : x_n) = F(y_0 : \dots : y_n)$ .

- **Injective?** Let  $(x_0 : \dots : x_n), (y_0 : \dots : y_n) \in \mathbb{P}_k^n$  be given. Then  $(x_0, \dots, x_n) \neq (0, \dots, 0)$  and  $(y_0, \dots, y_n) \neq (0, \dots, 0)$ . Suppose that  $F(x_0 : \dots : x_n) = F(y_0 : \dots : y_n)$ . Since  $(x_0, \dots, x_n) = (1x_0, \dots, 1x_n) \in F(x_0 : \dots : x_n) = F(y_0 : \dots : y_n)$ , there must exist a  $t \in k$  such that  $(x_0, \dots, x_n) = (ty_0, \dots, ty_n)$ . Since  $(x_0, \dots, x_n) \neq (0, \dots, 0)$ ,  $t \neq 0$ . Then  $t \in k^\times$ . Therefore,  $(x_0, \dots, x_n) = t * (y_0, \dots, y_n)$ , so  $(x_0 : \dots : x_n) = (y_0 : \dots : y_n)$ .
- **Surjective?** Let  $V$  be a one-dimensional subspace of  $k^{n+1}$ . Let  $\{(a_0, \dots, a_n)\}$  be a basis of  $V$ . Then  $V = \{(ta_0, \dots, ta_n) \mid t \in k\}$ . Since  $(a_0, \dots, a_n)$  is a basis element, it is nonzero. Therefore,  $(a_0 : \dots : a_n) \in \mathbb{P}_k^n$ . Then  $F(a_0 : \dots : a_n) = V$ .

$F$  is indeed a bijection between  $\mathbb{P}_k^n$  and the set of all one-dimensional subspaces of  $k^{n+1}$ .  $\square$

**Exercise.** (2.5) The set  $\pm 1$  is a group with group law given by multiplication. This group acts on the unit sphere,  $S^n := \{(x_0, \dots, x_n) \in \mathbb{R}^{n+1} : x_0^2 + \dots + x_n^2 = 1\}$  by scalar multiplication  $\pm 1 * (x_0, \dots, x_n) = \pm 1 \cdot (x_0, \dots, x_n)$ . Let  $\sim$  denote the corresponding equivalence relation on  $S^n$ . Construct a natural bijective map,  $S^n / \sim \rightarrow \mathbb{P}_{\mathbb{R}}^n$ .

*Proof.* Let  $f : S^n / \sim \rightarrow \mathbb{P}_{\mathbb{R}}^n$  be defined such that  $f([(x_0, \dots, x_n)]) = (x_0 : \dots : x_n)$ . We claim that  $f$  is a bijection.

- **Well-defined?** Let  $(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \in S^n$  be given. Since  $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$ , there exists a  $t \in \{-1, 1\}$  such that  $(x_0, \dots, x_n) = t \cdot (y_0, \dots, y_n) = (ty_0, \dots, ty_n)$ . Since  $t \in \mathbb{R}^*$ ,  $(x_0 : \dots : x_n) = (y_0 : \dots : y_n)$ . This implies that  $f([(x_0, \dots, x_n)]) = f([(y_0, \dots, y_n)])$ .
- **Injective?** Let  $(x_0, \dots, x_n), (y_0, \dots, y_n) \in S^n$  be given. Suppose  $f([(x_0, \dots, x_n)]) = f([(y_0, \dots, y_n)])$ . Then  $(x_0 : \dots : x_n) = (y_0 : \dots : y_n)$ . Therefore, there must exist a  $t \in \mathbb{R}^*$  such that  $(x_0, \dots, x_n) = (ty_0, \dots, ty_n)$ .

$$\begin{aligned} (ty_0)^2 + \dots + (ty_n)^2 &= t^2(y_0^2 + \dots + y_n^2) \\ &= t^2 \cdot 1 \\ &= t^2. \end{aligned}$$

On the other hand,  $x_0^2 + \cdots + x_n^2 = 1$ , so  $t^2 = 1$ . This implies that  $t \in \{-1, 1\}$ . Since  $(x_0, \dots, x_n) = t(y_0, \dots, y_n)$  for some  $t \in \{\pm 1\}$ ,  $[(x_0, \dots, x_n)] = [(y_0, \dots, y_n)]$  in  $S^n / \sim$ .

- Surjective? Let  $(x_0 : \cdots : x_n) \in \mathbb{P}_{\mathbb{R}}^n$ . Then  $(x_0, \dots, x_n) \neq 0$ , so  $x_0^2 + \cdots + x_n^2 \neq 0$ . Let  $c = x_0^2 + \cdots + x_n^2$ . Let  $y_i = x_i / \sqrt{c}$  for each  $i$ . This makes sense because  $c$  is a positive real number, so  $1/\sqrt{c}$  exists. Then  $y_0^2 + \cdots + y_n^2 = 1$ , so  $(y_0, \dots, y_n) \in S^1$ . Since  $\sqrt{c}(y_0, \dots, y_n) = (x_0, \dots, x_n)$ ,  $(y_0 : \cdots : y_n) = (x_0 : \cdots : x_n)$ . Therefore,  $f(y_0, \dots, y_n) = (x_0 : \cdots : x_n)$ , and thus  $f$  is indeed surjective.

□

### Exercise.

- Determine the number of elements in the group  $GL_2(R)$  when  $R$  is the ring  $\mathbb{Z}/p\mathbb{Z}$ , with  $p$  a prime number.
- $GL_2(\mathbb{Z}/p)$  acts on  $(\mathbb{Z}/p)^2$  by multiplying column vectors on the left by matrices. Determine the distinct orbits of this action.
- Describe the stabilizer subgroup in  $GL_2(\mathbb{Z}/p)$  of the element  $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \in (\mathbb{Z}/p)^2$ .

*Proof.*

- From linear algebra, we know that a matrix has a nonzero determinant if and only if the set of the column vectors is linearly independent. Since we are working with  $2 \times 2$  matrices here, it is equivalent to checking whether each vector is a scalar multiple of the other.
  - There are  $p^2 - 1$  columns that can be in an invertible matrix. This is because the only column vector that no invertible matrix has is the zero vector.
  - Suppose we pick one of the  $p^2 - 1$  columns as the left column vector. Then there are exactly  $(p^2 - 1) - (p - 1)$  column vectors that we can pick as the right column vector to create an invertible matrix. This is because any nonzero scalar multiple of  $p^2 - 1$  cannot be the right column vector, and if the right column vector is not a scalar multiple of the left vector, the matrix will be invertible.

Therefore, there are exactly  $(p^2 - 1)((p^2 - 1) - (p - 1)) = p^4 - p^3 - p^2 + p$  matrices in  $GL_2(R)$ .
- We claim that there are two distinct orbits. Let  $v = \begin{bmatrix} a \\ b \end{bmatrix} \in (\mathbb{Z}/p)^2$ .

- If  $v = 0$ , then the orbit is  $\{v\}$ .
- If  $v \neq 0$ , then we claim that the orbit is the collection of all the nonzero vectors. First, we claim that the column vector  $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$  is in the orbit of  $v$ .

$$* \text{ If } a \neq 0 \text{ and } b \neq 0, \text{ then } \begin{bmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

$$* \text{ If } a \neq 0 \text{ and } b = 0, \text{ then } \begin{bmatrix} a^{-1} & 0 \\ a^{-1} & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

$$* \text{ If } a = 0 \text{ and } b \neq 0, \text{ then } \begin{bmatrix} 1 & b^{-1} \\ 0 & b^{-1} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

Since this argument can be applied to any nonzero column vector, it implies that the orbit of any nonzero column vector contains  $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ . Since the orbits are equivalence classes, they are either disjoint or identical. In other words, this implies that every nonzero column vector has the same orbit.

Moreover, for any  $w \in (\mathbb{Z}/p)^2$ ,  $Iw = w$  where  $I$  denote the identity matrix. Thus the orbit of a nonzero vector contains any nonzero vector.

Therefore, the orbit of any nonzero vector is the set of all the nonzero vectors.

•

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \implies \begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Therefore, it suffices to determine what the values of  $b$  and  $d$  are.  $\begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix}$  is an upper triangular matrix, so it is invertible if and only if  $d \neq 0$ . Therefore,

$$G \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \left\{ \begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix} \mid b, d \in \mathbb{Z}_p, d \neq 0 \right\}.$$

□