411 Individual HW4

Jack Madden

October 2023

Problem 1

a)

D_3	S_3
Id	Id
Rot 120	(123)
Rot 240	(132)
Refl 1	(23)
Refl 2	(13)
Refl 3	(12)

b)

${\mathbb{Z}_5}^*$	S_4
1	Id
2	(1234)
3	(1432)
4	(13)(24)

The idea here is that we first recognize that there is an isomorphism between $\mathbb{Z}_4$ and a subgroup of S_4, which corresponds to the permutations which shift elements by the numbers in $\mathbb{Z}_4$, and that there is an isomorphism between ${\mathbb{Z}_5}^*$ and $\mathbb{Z}_4$ because ${\mathbb{Z}_5}^*$ is cyclic and generated by 2. We then chain these two isomorphisms to generate an isomorphism between $\mathbb{Z}_5$ and a subgroup of S_4.

Problem 2

a) Let's call the isomorphism $\phi : G \to H$. Choose arbitrary $a, b \in G$. Then these are mapped to $\phi(a), \phi(b) \in H$. Then:

$$\phi(ab) = \phi(a) \cdot \phi(b)$$

But then, since G is Abelian and thus $ab = ba$ and ϕ is a well defined function:

$$\phi(ab) = \phi(ba) = \phi(a) \cdot \phi(b)$$

$$\phi(ab) = \phi(b) \cdot \phi(a) = \phi(a) \cdot \phi(b)$$

So clearly for any $\phi(a) = y_1, \phi(b) = y_2 \in H, y_1 y_2 = y_2 y_1$ and H is Abelian.

b) Let's call the n elements of order d in G, $S = a_1, a_2, a_3, \cdots, a_n$. Then there is a set of elements $T = \phi(a_1), \phi(a_2), \phi(a_3), \cdots, \phi(a_n) \in H$. Take an element $a_i \in S$. Then, since $a_i^d = a_i^{d-1} a_i$:

$$\phi(a_i^{d-1} a_i) = \phi(a_i^{d-2} a_i) \cdot \phi(a_i)$$

We can recursively apply this property and observe that:

$$\phi(a_i^d) = \phi(a_i)^d$$

But since $\phi(a_i^d) = \phi(e_G)$ and an isomorphism must map one identity to the other, we have $\phi(a_i)^d = e_H$. We can show that d is the order of $\phi(a_i)$ by contradiction. Assume there exists $0 < k < d$ such that $\phi(a_i)^k = e_H$. But then $\phi(a_i)^k = \phi(a_i^k)$, and since a_i^k cannot be e_G given the constraints on k, $\phi(a_i)^k$ cannot be e_H. Contradiction. So all elements a_i of order d in G have a corresponding element $\phi(a_i)$ of order d in H. So it's clear that H has at least n elements of order d. Assume then that there is an additional element $\phi(b) \in H$, $ord(b) \neq d, ord(\phi(b)) = d$. Let the order of b be $\ell \neq d$ So then:

$$\phi(b)^d = \phi(b^d) = e_H$$

We break this down into 3 cases.

Case 1: $\ell > d$:

In this case, $b^d \neq e_G$ and thus $\phi(b)^d = \phi(b^d) \neq e_H$.

Case 2: $\ell < d, \ell \nmid d$ In this case $d = \ell q + r$, $r, q \in \mathbb{Z}$, $0 < r < \ell$.

Then:

$$\phi(b)^d = \phi(b^d) = \phi(b^{\ell q+r}) = \phi(b^{lq})\phi(b^r) = \phi(e_G)\phi(b^r) = \phi(b^r)$$

But based on the constraints placed on r, b^r cannot be e_G, so $\phi(b^r) \neq e_H$.

Case 3: $\ell < d, \ell | d$

Let $d = \ell q$, $q \in \mathbb{Z}^+$ Then:

$$\phi(b)^d = \phi(b^d) = \phi(b^{\ell q}) = \phi((b^\ell)^q) = \phi(b^\ell)^q$$

But then we observe that $\phi(b^\ell) = e_H$ and so order $\phi(b)$ is $\ell \neq d$.

Problem 3

a) G has order $3! = 6$. So if it were isomorphic to a subgroup of $\mathbb{Z}_{60}$, it would need to be isomorphic to $\langle 10 \rangle$ as $|\langle 10 \rangle|$ is 6. Suppose an isomorphism ϕ exists between S_3 and $\langle 10 \rangle$. We notice that S_3 has 3 elements of order 2, namely the transpositions $(12), (13), (23)$. However, only 1 element in $\langle 10 \rangle$ has order 2, 30. Based on the contrapositive of what was shown in Problem 2, this isomorphism cannot exist.

b) Suppose an isomorphism ϕ exists between $\mathbb{Z}_8$ and S_7. Take the element 1 in Z_8. We know that 1 has order 8 in $\mathbb{Z}_8$ and thus there must be a corresponding element of order 8 in S_7. Let's look at the orders of elements in S_7 by decomposing the ways permutations can be written in disjoint cycles. $(abcdefg)$: order 7, $(abcdef)$: order 6, $(abcde)$: order 5, $(abcd)$: order 4, (abc): order 3, (ab): order 2, $(abcde)(fg)$: order 10, $(abcd)(efg)$: order 12, $(abcd)(ef)$: order 4, $(abc)(def)$: order 3, $(abc)(de)$: order 6, $(abc)(de)(fg)$: order 6, $(ab)(cd)$, order 2, $(ab)(cd)(ef)$, order 2. Thus there is no corresponding element with order 8 and $\mathbb{Z}_8$ cannot be isomorphic to any subgroup of S_7.

c) Every element in $\mathbb{Z}_8^*$ has order 2, however only one element in $\mathbb{Z}_{24}$ has order 2, 12. Thus based on the contrapositive of what was shown in Problem 2 no isomorphism exists.

Problem 4

a) a

b) We first observe that when x is a reflection, x^2 will simply be the identity, and when x is a rotation, if x_i is the i^{th} rotation (0-indexed) by 36 degrees, than x_i^2 is $x_{2i \bmod 10}$. So the rotations which are square are those which can be written as $2i - 10q$, $q = 0, 1$. Factoring out 2 we find that $2(i - 5q)$ and conclude that only the even rotations in D_{10} are square.

c) We contend that all elements are square. We represent the i^{th} even number as 2i, and the i^{th} odd number as $2i - 1$. We notice that the result of $x + x$, $x \in \mathbb{Z}_{2021}$ mod 2021 is $(x + x) - 2021q$, where $q = 0, 1$. We observe that the i^{th} even number can simply be written as $i + i - 2021 \cdot 0$, and the i^{th} odd number can be written as:

$$(i + 1010) + (i + 1010) - 2021$$

$$2i + 2020 - 2021$$

$$2i - 1$$

So all elements of $\mathbb{Z}_{2021}$ are square.

Problem 6

a) We have the following types of cycles:

$$(a\ b\ c\ d\ e)$$

$\frac{5!}{5} = 24$ such cycles exist, and these cycles have order 5.

$$(a\ b\ c\ d)$$

$\frac{5!}{4} = 30$ such cycles exist, and these cycles have order 4.

$$(a\ b\ c)$$

$\frac{5 \cdot 4 \cdot 3}{3} = 20$ such cycles exist, and they have order 3.

$$(a\ b\ c)(d\ e)$$

$\frac{5!}{3 \cdot 2} = 20$ such cycles exist and these cycles have order $lcm(3,2) = 6$.

$$(a\ b)(c\ d)$$

$\frac{5!}{2 \cdot 2 \cdot 2} = 15$ such cycles exist, and these cycles have order $lcm(2,2) = 2$.

$$(a\ b)$$

$\frac{5 \cdot 4}{2} = 10$ such cycles exist, and they have order 2.
Then there is the identity permutation with order 1 and we have described all types of disjoint cycle decompositions.

b) b

c) For reflections, we see we have two types. The first type is those reflections which keep two points e, f. These reflections have the form $(a\ b)(c\ d)$. 3 such reflections exist and their order is 2. The second type is reflections which have 3 exchanges of pairs of points. These reflections have the form $(a\ b)(c\ d)(e\ f)$. The reflection of 4 turns also has this form as its decomposition is (1 4)(2 5)(3 6) and so there are 4 elements that have this disjoint cycle decomposition. These permutations have order 2.
We now examine the rotations.
The rotation by 1 turn is (1 2 3 4 5 6). The rotation by 5 turns is (1 6 5 4 3 2).
Thus there are 2 such permutations of the form $(a\ b\ c\ d\ e\ f)$ and they have order 5.
The rotation by 2 turns is (1 3 5)(2 4 6). The rotation by 4 turns is (1 5 3)(2 6 4).
Thus there are 2 such permutations of the form $(a\ b\ c)(d\ e\ f)$ and they have order 3.

Problem 7

a) $\phi(x) = gx$ is only an isomorphism when $g = e$. When $g = e$, $\phi(x) = x$. Clearly this is a one to one function and we can see that it satisfies the property of isomorphism.

$$\phi(x_1 x_2) = \phi(x_1)\phi(x_2)$$
$$x_1 x_2 = x_1 x_2$$

. However, let $g \neq e$. Let's check the property of isomorphism when $x_1, x_2 = e$.

$$\phi(x_1 x_2) = \phi(x_1)\phi(x_2)$$
$$\phi(ee) = \phi(e)\phi(e)$$
$$\phi(e) = \phi(e)\phi(e)$$
$$g = gg$$
$$g^{-1}g = g^{-1}gg$$
$$e = g$$

And we have a contradiction.

b) $\phi(x) = gxg^{-1}$ is always an isomorphism. We check that ϕ is one to one. Let $\phi(x_1) = \phi(x_2)$

$$\phi(x_1) = \phi(x_2)$$
$$gx_1g^{-1} = gx_2g^{-1}$$
$$g^{-1}gx_1g^{-1}g = g^{-1}gxg^{-1}g$$
$$ex_1e = ex_2e$$
$$x_1 = x_2$$

We then verify that $\phi(x_1 x_2) = \phi(x_1)\phi(x_2)$ for any $x_1, x_2 \in G$.

$$\phi(x_1 x_2) = \phi(x_1)\phi(x_2)$$
$$gx_1x_2g^{-1} = gx_1g^{-1}gx_2g^{-1}$$
$$gx_1x_2g^{-1} = gx_1x_2g^{-1}$$

Problem 8

a) Without loss of generality assume $a < b$. We propose that (a b) can be written as the product of the adjacent transpositions:

$$(a\ a+1)(a+1\ a+2)\cdots(b-2\ b-1)(b-1\ b)(b-1\ b-2)\cdots(a+2\ a+1)(a+1\ a)$$

We observe that the product of the center 3 transpositions is $(b-2\ b)$ giving us

$$(a\ a+1)\cdots(b-3\ b-2)(b-2\ b)(b-2\ b-3)\cdots(a+1\ a)$$

Intuitively this process maps the elements $(a+1\ b-1)$ to themselves in reverse while incrementally moving a, b towards each other. We finally get

$$(a\ a+1)(a+1\ b)(a+1\ a)$$

which gives us our final transposition $(a\ b)$

b) We have proved that any transposition in S_n can be written as a product of the adjacent transpositions in S_n, and we know that any permutation in S_n can be written as the product of transpositions. Thus transitively we can see that any $\sigma \in S_n$ can be written as the product of adjacent transpositions and thus the set $(1\ 2), (2\ 3)\cdots, (n-1\ n)$ is generating.

Problem 9

To prove this we'll break elements of S_n into two classes and evaluate $\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1}(t)$, $t \in S_n$.

Case 1, t such that $\sigma^{-1}(t) \notin \{i_1, i_2, \cdots, i_k\}$:

In this case, $t \xrightarrow{\sigma^{-1}} \sigma^{-1}(t) \xrightarrow{(i_1,i_2,\cdots,i_k)} \sigma^{-1}(t) \xrightarrow{\sigma} t$.

Case 2 t such that $\sigma^{-1}(t) \in \{i_1, i_2, \cdots, i_k\}$:

In this case it is more complicated to evaluate. Let $\sigma^{-1}(t) = i_m \in \{i_1, i_2, \cdots, i_k\}$. First t is moved to $\sigma^{-1}(t) = i_m$. i_m is then moved to i_{m+1} which is moved to $\sigma(i_{m+1})$. But since $\sigma^{-1}(t) = i_m$, $t = \sigma(i_m)$ and thus $\sigma(i_m)$ is moved to $\sigma(i_{m+1}$ yielding the cycle $(\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$. Since the elements in case 1 are simply moved to themselves, we have $\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$.