MATH 411: INTRODUCTION TO ABSTRACT ALGEBRA
HOMEWORK #4

TRUNG DANG
33858723

Problem 1

Problem Statement: Describe explicitly an isomorphism of each of the following groups with a subgroup of a symmetric group given by the Cayley Theorem. In other words, for each element of the group, list the corresponding permutation:

(1) D_3

(2) $\mathbb{Z}_5^*$

Solution. (1) Denote R as the rotation counterclockwise by 120 degrees and S as the symmetry by vertex 1. We have the following multiplication table, If we assign each element

	Id	R	R^2	S	RS	R^2S
Id	Id	R	R^2	S	RS	R^2S
R	R	R^2	Id	RS	R^2S	S
R^2	R^2	Id	R	R^2S	S	RS
S	S	R^2S	RS	Id	R^2	R
RS	RS	S	R^2S	R	Id	R^2
R^2S	R^2S	RS	S	R^2	R	Id

of D_3 to a number from 1 to 6, respectively, then by Cayley Theorem, D_3 is isomorphic to a subgroup of S_6 by the following mapping:

$$Id \mapsto \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}$$

$$R \mapsto \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{bmatrix}$$

$$R^2 \mapsto \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{bmatrix}$$

$$S \mapsto \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{bmatrix}$$

$$RS \mapsto \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 1 & 2 \end{bmatrix}$$

$$R^2S \mapsto \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 3 & 1 \end{bmatrix}$$

(2) we have the following multiplication table, So $\mathbb{Z}_5^*$ is isomorphic to a subgroup of S_4, by a

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

bijection f that maps:

$$\begin{aligned} &1 \to Id \\ &2 \to (1243) \\ &3 \to (1342) \\ &4 \to (14)(23) \end{aligned}$$

$\blacksquare$

Problem 2

Problem Statement: Let G and H be isomorphic groups. Prove the following statements:

(1) If G is abelian then H is abelian

(2) If G has n elements of order d then H has n elements of order d

Solution. (1) If G and H are isomorphic then there must be a bijection $f : G \to H$ such that $f(x \circ y) = f(x) \cdot f(y)$
Therefore, if G is Abelian, then for any $a, b \in H$,

$$\begin{aligned} a \cdot b &= f(f^{-1}(a)) \cdot f(f^{-1}(b)) \\ &= f(f^{-1}(a) \circ f^{-1}(b)) \\ &= f(f^{-1}(b) \circ f^{-1}(a)) \\ &= f(f^{-1}(b)) \cdot f(f^{-1}(a)) = b \cdot a \end{aligned}$$

Therefore, H is a group and H is commutative for all a, b in H. Therefore H is abelian.

(2) We will prove that f maps an element of order d from G to an element of order d in H. Indeed, for all element a, $f(a) = f(a \circ e) = f(a) \cdot f(e)$. So $f(e)$ is the identity of H, or f maps identity to identity.
For every $g \in G$, $ord(g) = d$, then $f(e) = f(\underbrace{g \cdot g \cdot g \cdots g}_{\text{d times}}) = \underbrace{f(g) \cdots f(g)}_{\text{d times}}$
Therefore the order of $f(g)$ is at most d. (1)
Assume that the order of $f(g)$ is $k < d$ instead, then $f(e) = \underbrace{f(g) \cdots f(g)}_{\text{k times}} = f(\underbrace{g \cdot g \cdots g}_{\text{k times}})$,
hence $e = g^k$, or the order of g is at most $k < d$, which is a contradiction. (2).

From (1) and (2), we can conclude that f maps an element of order d to an element of order d. And since f is a bijection, the number of elements of a specific order d of H and G must be equal

■

Problem 3

Problem Statement: For each of the following pairs of groups G and H, prove that G is not isomorphic to a subgroup of H.

(1) $G = S_3, H = \mathbb{Z}_{60}$

(2) $G = \mathbb{Z}_8, H = S_7$

(3) $G = \mathbb{Z}_8^*, H = \mathbb{Z}_{24}$

Solution. (1) Consider the following permutations in S_3: $(12), (23), (31)$. They are all transpositions and they are of order 2. Therefore, by *Problem 2*, in order for G to be isomorphic to a subgroup of H, then this subgroup must have at least 3 elements of order 2. However, in the entirety of $\mathbb{Z}_{60}$ there is only 1 element of order 2, namely 30.
Therefore, G is not isomorphic to any subgroup of H

(2) Consider the number 3. The order of 3 in $\mathbb{Z}_8$ is 8. We will show that all elements of S_7 cannot be of order 8.
Indeed, since every permutation can be partitioned into disjoint cycles and the order of a permutation is the L.C.M. of the length of the cycles, we shall list all the possible partitioning here:

PARTITIONING	ORDER
7+0	7
6+1	6
5+2	10
5+1+1	5
4+3	12
4+2+1	4
4+1+1+1	4
3+3+1	3
3+2+2	6
3+2+1+1	6
3+1+1+1+1	3
2+2+2+1	2
2+2+1+1+1	2
2+1+1+1+1+1	2
1+1+1+1+1+1+1	1

Since none of the elements of S_7 has order 8, it can have no subgroup with an element of order 8. So $\mathbb{Z}_8$ is not isomorphic to a subgroup of H

(3) Consider $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod 8$.
In G, there are at least 3 elements (namely, 3,5,7) of order 2. However, the only element of order 2 in $\mathbb{Z}_{24}$ is 12. Therefore, $\mathbb{Z}_{24}$ cannot have any subgroup with 3 elements of order 2.
Hence, G is not isomorphic to any subgroup of H.

■

Problem 4

Problem Statement: An element x of a group G is called a square if $x = y^2$ for some $y \in G$. Find all squares in the following groups:

(1) S_4

(2) D_{10}

(3) $\mathbb{Z}_{2021}$

Solution. (1) For brevity, the set below is only the lower row of the permutation. For example, I listed the permutation: $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$ as $\{2,3,4,1\}$. Then, the list of all squares in S_4 is:

$\{\{1,2,3,4\},\{1,4,2,3\},\{1,3,4,2\},\{3,1,2,4\},\{3,4,1,2\},\{4,3,2,1\},\{4,1,3,2\},\{2,3,1,4\},\{4,2,1,3\},$
$\{2,1,4,3\},\{2,4,3,1\},\{3,2,4,1\}\}$

Rationale: This is the code that I used in Wolfram Mathematica to generate the list of all squares of S_4:

```
perms = Permutations[Range[4]];
squares = PermutationCompose[#, #] & /@ perms;
uniqueSquares = DeleteDuplicates[squares];
uniqueSquares
```

(2) $\{Id, R^2, R^4, R^6, R^8\}$
Rationale: For every rotation by $\frac{k2\pi}{10}$ degrees, its square is the rotation by $\frac{2k2\pi}{10}$. And because 10 is even, $2k$ is equivalent to some even numbers modulo 10, hence the only rotations that are squares in D_10 are Id, R^2, R^4, R^6, R^8.
For every reflection, its square is the identity operation.
Therefore, the list of all squares in D_10 is $\{Id, R^2, R^4, R^6, R^8\}$

(3) $\mathbb{Z}_{2021}$
We will show that every number $k \in \mathbb{Z}_{2021}$ is a square in $\mathbb{Z}_{2021}$.
Indeed, if k is even, that is $k = 2s$, then $k \equiv 2 \cdot s \mod 2021$. (1)
Else, if $k = 2s+1$, then $k \equiv 2021 + 2s + 1 \equiv 2(s+1011)$. But since $k = 2s+1 < 2021$, then $s < 1010$. So $s + 1011 < 2021$, hence k is a square. (2)
From (1) and (2), every element of $\mathbb{Z}_{2021}$ is a square

■

Problem 5

Problem Statement: Use Mathematica to draw a histogram of all possible orders in groups

(1) S_7

(2) S_8

(3) S_9

For each of the groups, answer the following questions:

- What is the maximal possible order and how often does it appear?
- What is the most frequent order and how often does it appear?

Merge the PDF file of your Wolfram Cloud code and output with your homework file. In addition, provide a link to your Wolfram Cloud code.

Solution. Link to Wolfram Mathematica Code:
https://www.wolframcloud.com/env/tmdang/TrungDangHW4.5.nb

(1)
- The maximal order is 12 and it appears 420 times
- The most frequent order is 6 and it appears 1470

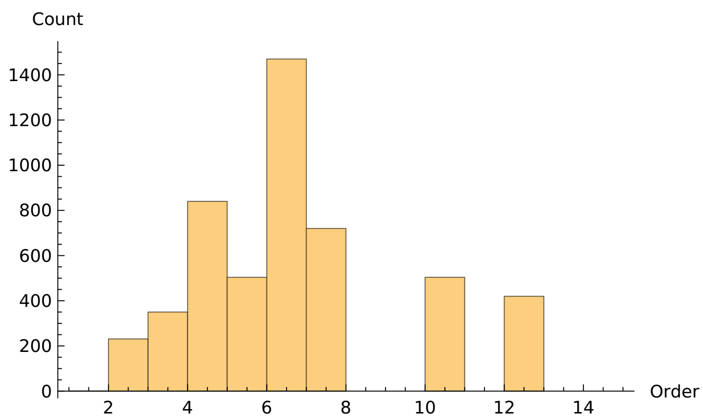
(2)
- The maximal order is 15 and it appears 2688 times
- The most frequent order is 6 and it appears 10640 times

(3)
- The maximal order is 20 and it appears 18144 times
- The most frequent order is 6 and it appears 83160 times

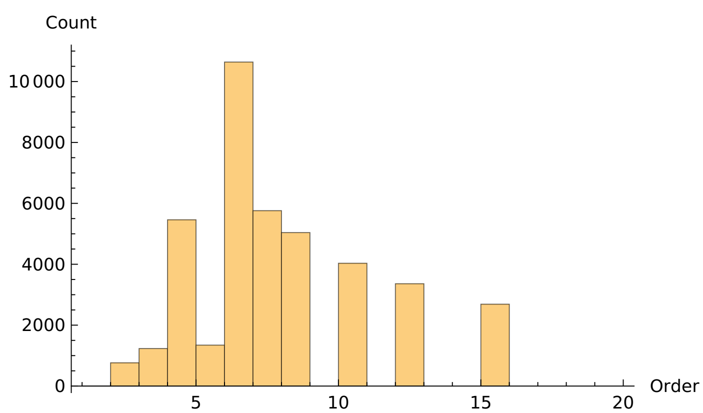
∎

In[40]:=
```
perms = Permutations[Range[7]];
orders = PermutationOrder /@ perms;
Histogram[orders, {1, 15, 1}, AxesLabel → {"Order", "Count"}]
perms = Permutations[Range[8]];
orders = PermutationOrder /@ perms;
Histogram[orders, {1, 20, 1}, AxesLabel → {"Order", "Count"}]
perms = Permutations[Range[9]];
orders = PermutationOrder /@ perms;
Histogram[orders, {1, 24, 1}, AxesLabel → {"Order", "Count"}]
```

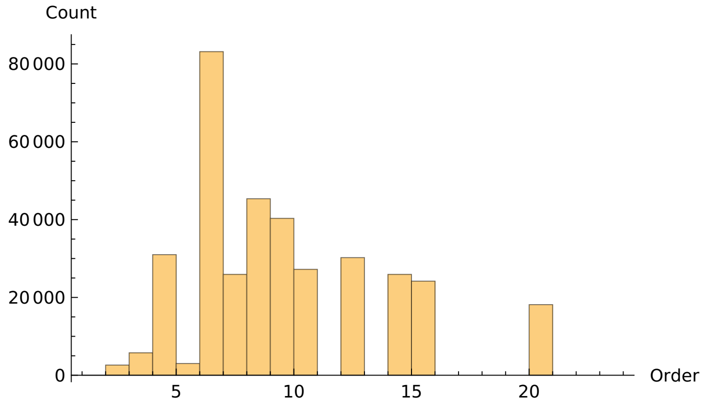
Out[42]=



Out[45]=



Out[48]=



Problem 6

Problem Statement: Find all possible types of disjoint cycles decompositions of permutations from the following groups:

(1) S_5

(2) S_6

(3) $D_6 \subset S_6$

For each type, compute the order of a permutation.

Solution. We again note that each permutation can be represented as a product of disjoint cycles (some of which may be of length 1, which preserves the position of the element). Also, note that the order of a permutation is the L.C.M of the lengths of the cycles.

(1) The possible cycle decompositions, an example, and their respective orders are:

Types	Example	Order
5+0	(12345)	5
4+1	(1234)	4
3+2	(123)(45)	6
3+1+1	(123)	3
2+2+1	(12)(34)	2
2+1+1+1	(12)	2
1+1+1+1+1	Id	1

(2) The possible cycle decompositions, an example, and their respective orders are:

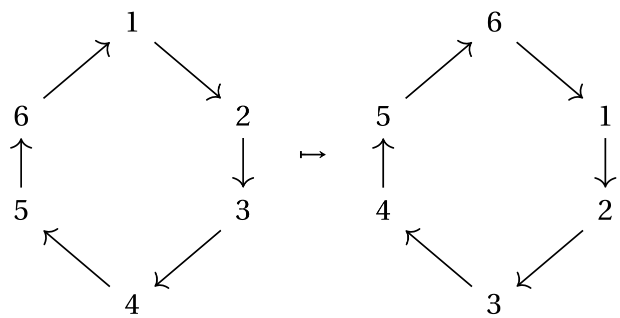
Types	Example	Order
6+0	(123456)	6
5+1	(12345)	5
4+2	(1234)(56)	4
4+1+1	(1234)	4
3+3	(123)(456)	3
3+2+1	(123)(45)	6
3+1+1+1	(123)	3
2+2+2	(12)(34)(56)	2
2+2+1+1	(12)(34)	2
2+1+1+1+1	(12)	2
1+1+1+1+1+1	Id	1

(3) For elements in $D_6 \subset S_6$, there can be only 2 types of cycles decomposition:

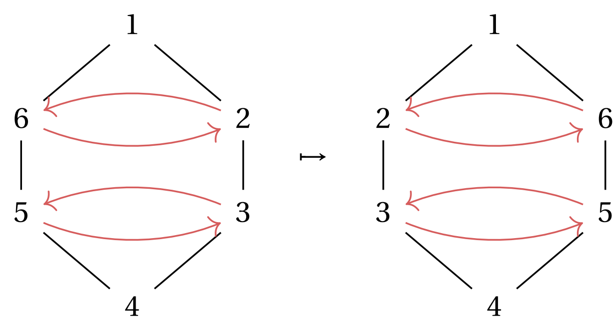
- One cycle of length 6 for some rotation

- 2 cycles of length 2 and 2 "cycles" of length 1 for some reflection

In the first case, all 6 vertices form a cycle, for an order of 6



In the second case, 2 vertices on the axis preserves their positions, and vertices symmetric to the axis swap places with each other, forming 2 transpositions (or 2 cycles of length 2). The cycle decomposition as a whole has an order of 2



■

Problem 7

Problem Statement: Let G be a group and fix an element $g \in G$. Consider the following functions from G to G.

(1) x is sent to gx. (this is called a left translation by g)

(2) x is sent to gxg^{-1} (this is called a conjugation by g)

Prove that one of these functions is always an isomorphism but another is an isomorphism only if $g = e$

Solution. We will prove that (2) is an isomorphism regardless of g but (1) is an isomorphism only if $g = e$.
Indeed, we first show that both (1) and (2) are bijections from G to G. In fact, let $f(x) = gx$.
Assume $f(x) = f(y)$ for some x, y, then left multiply both sides by g^{-1} we have $g^{-1}gx = g^{-1}gy$, thus $x = y$.
Furthermore, $x = g(g^{-1}x), \forall x \in G$.
Therefore, $f : G \to G$ is a bijection.
Similarly, let $h(x) = gxg^{-1}$.
Assume $h(x) = h(y)$ for some x, y, Then, $g^{-1}h(x)g = g^{-1}h(y)g$ yields $x = y$.
Also, $x = g^{-1}xg, \forall x \in G$.
Therefore, $h : G \to G$ is a bijection.

Now, assume that f is an isomorphism. That means, $\forall x, y \in G$:

$$f(x \cdot y) = f(x) \cdot f(y)$$

, or

$$\begin{aligned}
&gxy = gxgy \\
\Longrightarrow\, &g^{-1}gxy = g^{-1}gxgy \\
\Longrightarrow\, &xy = xgy \\
\Longrightarrow\, &xyy^{-1} = xgyy^{-1} \\
\Longrightarrow\, &x = xg \\
\Longrightarrow\, &g = e
\end{aligned}$$

Reversely, if $g = e$ then $f(x) = gx$ is the identity function, and therefore is an isomorphism.
Meanwhile,

$$\begin{aligned}
h(x \cdot y) &= gxyg^{-1} \\
&= gxeyg^{-1} \\
&= gxg^{-1}gyg^{-1} \\
&= (gxg^{-1})(gyg^{-1}) \\
&= h(x) \cdot h(y)
\end{aligned}$$

Therefore, h is an isomorphism regardless of g.
In conclusion, (2) is always an isomorphism but (1) is an isomorphism only if $g = e$ ∎