MATH 411: INTRODUCTION TO ABSTRACT ALGEBRA
HOMEWORK #3

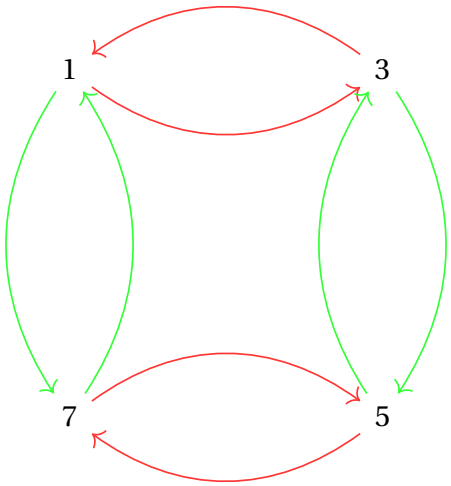
TRUNG DANG
33858723

Problem 1: For each of the following groups, decide if it has a generator. If not, prove why not. If yes, list all possible generators: (a) $\mathbb{Z}_6$ (b) $\mathbb{Z}_{11}^*$ (c) $\mathbb{Z}_{14}^*$

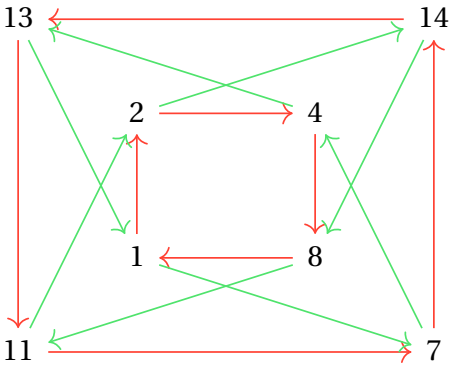
Solution. (a) $\mathbb{Z}_6$ has a generator. The generators are $\boxed{\text{1 and 5}}$. 2 cannot be a generator for it will only yield remainders $0,2,4$. Similarly, 0 will only give 0, 3 will only give $0,3$, and 4 will only give $0,2,4$
(b) $\mathbb{Z}_{11}^*$ has generators. For a number a to be a generator of $\mathbb{Z}_{11}^*$, then $ord(a) = \varphi(11) = 10$ We can verify that all possible elements are $\boxed{\text{2,6,7,8}}$
(c) $\mathbb{Z}_{14}^*$ has generators. For a number a to be a generator of $\mathbb{Z}_{14}^*$, $ord(a) = \varphi(14) = 6$. All the possible elements are: $\boxed{\text{3 and 5}}$ ■

Problem 2: Show that each of the following groups has a generating set with 2 elements. Use your generating sets to draw the Cayley graphs of these groups: (a) $\mathbb{Z}_8^*$; (b) $\mathbb{Z}_{15}^*$

Solution. (a) The generating set is: $\{3,7\}$, The red arrows represent operation with 3, the green arrows represents operation with 7



(b) The generating set is $\{2,7\}$. The red arrows represent operations with 2, the green arrows represents the operation with 7



■

Problem 3: (a) Show that D_5 does not have a generating set that consists of 2 rotations. (b) Show that D_5 has a generating set that consists of 2 reflections. Draw the corresponding Cayley graph.

Solution. (a) Define two edges of a pentagon to be adjacent if they are connected by 2 edges of the pentagon. Then, any rotation preserves the adjacency of 2 points on a pentagon, that is: 2 vertices will be adjacent after a rotation if and only if they were adjacent before the rotation is applied.
Moreover, any rotation preserves the order of 2 adjacent elements, i.e. if 2 follows 1 in counterclockwise order before the rotation, then 2 also follows 1 in counterclockwise order after the rotation.

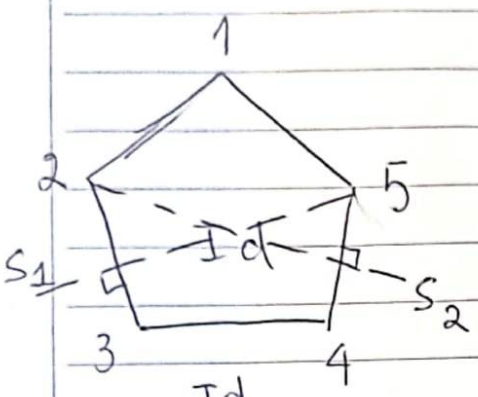
Therefore, any combination of 2 rotations will not be able to generate;

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

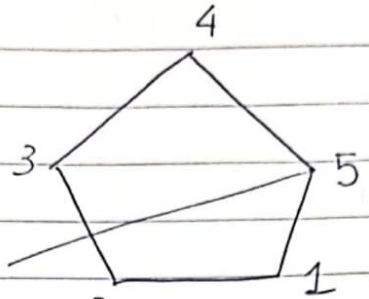
, which is the reflection across vertex 1.
Hence, D_5 does not have a generating set that consists of 2 rotations.

(b) Denote S_1 as the symmetry across vertex 5, and S_2 be the symmetry across vertex 2. Denote R to be the counterclockwise rotation of 72 degrees.
Then, $\{S_1, S_2\}$ generates D_5 as follows

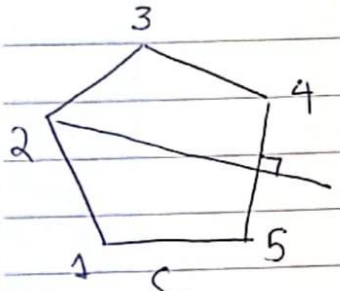
Thứ ngày . .



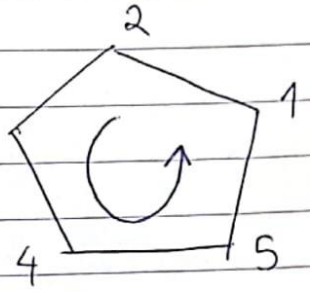
Id



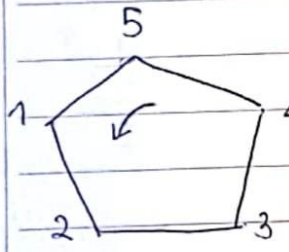
S_1



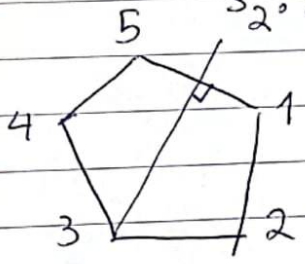
S_2



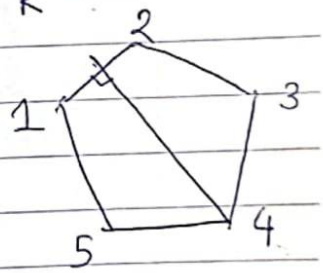
$S_2 \circ S_1 = R^4$



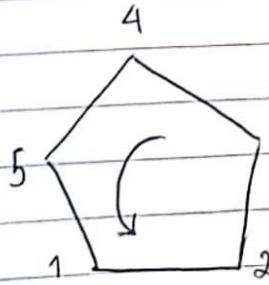
$S_1 \circ S_2 = R$



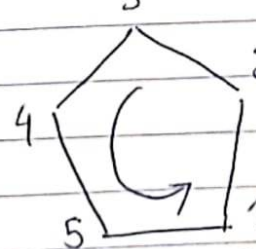
$S_1 \circ S_2 \circ S_1 =$ = reflection across 3.



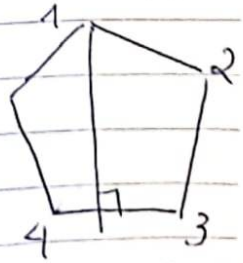
$S_2 \circ S_1 \circ S_2$ = reflection across 4.



$S_1 \circ S_2 \circ S_1 \circ S_2 = R^2$.

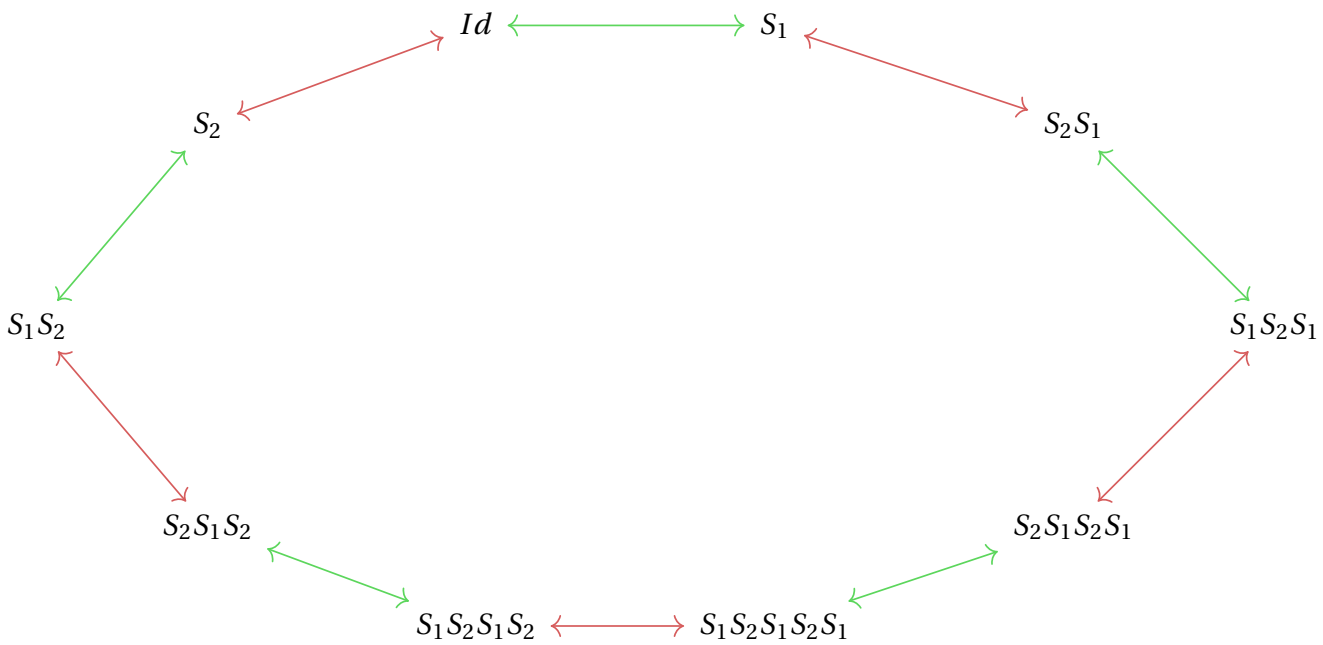


$S_2 \circ S_1 \circ S_2 \circ S_1 = R^3$

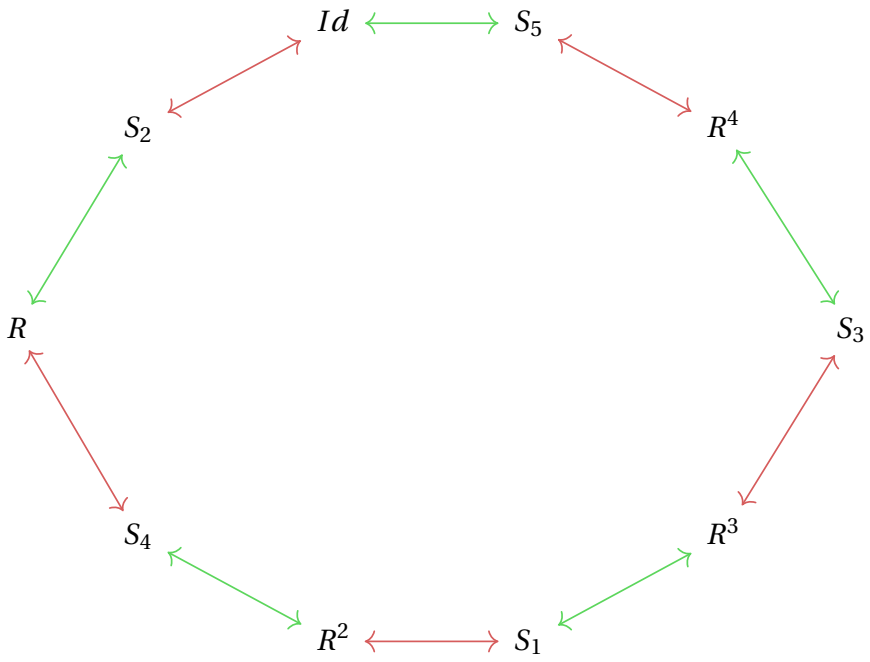


$S_1 \circ S_2 \circ S_1 \circ S_2 \circ S_1$ = reflection across 1.

Then, let the green arrows denote operation with S_1, and the red arrows denote operation with S_2, the Cayley Graph will be:



For brevity, let us relabel the elements of the Dihedral group as follows: R^n will be the rotation by 72 degrees n times, and S_n will be the reflection around vertex n. Then,



■

Problem 4: Let $2^{\{1,2,3\}}$ be the power set with the binary operation $(A \cup B) \setminus (A \cap B)$.
(a) Show that this group does not have a generating set with two elements.
(b) Show that this group has a generating set with three elements and draw the Cayley graph in such a way that the arrows do not intersect.

Solution. First, observe that the binary operation translates to $x \in A \bigoplus x \in B$, where the $\bigoplus$ notation is the XOR operator, and we write in short $A \triangle B$.
We will show that $\triangle$ is commutative, the group identity is $\emptyset$, and the inverse of each element is itself.

(1) for an element x and 2 subsets A, B of $\{1,2,3\}$; If x is in exactly one of A or B then it is also in either B or A but not both. Therefore, $A \triangle B = B \triangle A$.

(2) Second, $A \triangle \emptyset$ is the set of elements in either A or $\emptyset$, which is A.

(3) Third, $A \triangle A$ is the set of all elements in A or A but not both, so $A \triangle A = \emptyset$

We will use these three properties to prove (a)
(a) Assume the contrary, that the power set does have a generating set of two elements: $\{A, B\}$.
We will prove that the number of elements generated by this set is less than 8, the total number of elements of the power set.
Indeed, for each sequence of generators:

$$AABBAA \cdots ABA$$

We can use result (1) to "swap" A's and B's such that all A's are followed by all B's. So all strings of generating operations can be converted to:

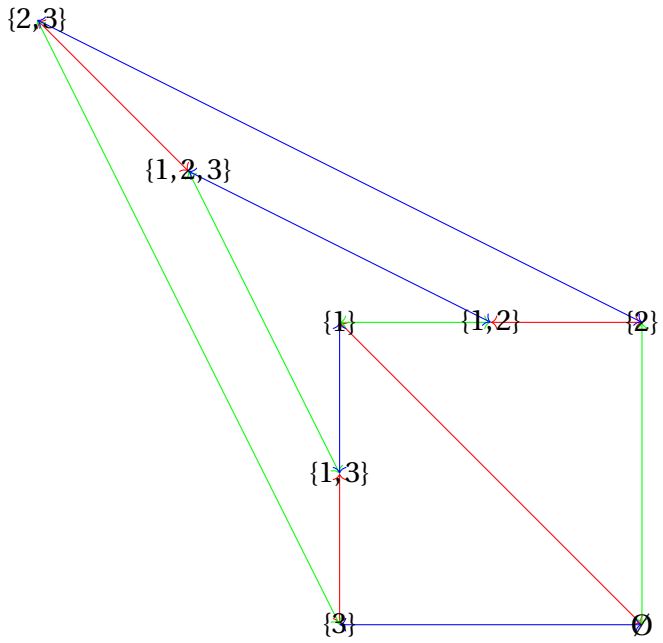
$$AAAA \cdots AABBB \cdots BB$$

Using result (3), we can see that strings of an odd number of A's is actually equal to A:

$$\underbrace{AAA \cdots A}_{2k+1 \text{ times}} = A \triangle (\underbrace{(AA)(AA) \cdots (AA)}_{k \text{ times}}) = A \triangle \underbrace{\emptyset\emptyset \cdots \emptyset}_{k \text{ times}} = A$$

Similarly, an even number of A's equal to $\emptyset$, and odd number of B's equal to B, an even number of B's equal to $\emptyset$.
Therefore, for all A, B, we can generate at most $2 \times 2 = 4$ sets, which is less than the number of elements in the power set of $\{1,2,3\}$. So the assumption is false, and the proof is complete.

(b) The generating set with three elements is : $\{\{1\},\{2\},\{3\}\}$. The Cayley graph below illustrates how to construct the group, wherein the red line corresponds to $\{1\}$, the green line corresponds to $\{2\}$, and the blue line corresponds to $\{3\}$:



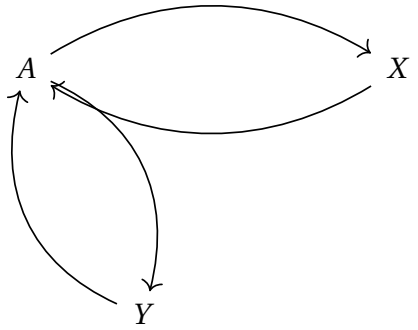
■

Problem 5: Take two vertices in the Cayley graph of some finite group. Prove that there always exists a sequence of arrows connecting these vertices. If you can't prove this in general, explain why this fact holds in the example of the Cayley graph of Problem 4, for partial credit.

Solution. We prove this using the following lemmas: (1) if from a generating element A we can reach X, then we can also reach A from X (that is, they will complete a full cycle), (2) from each generating element A we can reach all other elements of the group only using operations on generating elements.

(1) Let $X = A \cdot \sigma$. Then σ is the result of a sequence of generating operators. By definition of the generating set, σ^{-1} must also be represented by another sequence of generating operators (i.e. arrows in the Cayley graph). Therefore, $X \cdot \sigma^{-1} = A \cdot \sigma \cdot \sigma^{-1} = A$

(2)



Similarly, let $Y = A\varphi$, wherein φ is also a member of the group. Then by definition of the generating set, φ can be expressed as the composition of multiple operations on generating elements (i.e. arrows on the Cayley graph). Therefore, there exists a sequence of arrows $A \to Y$.

Using the aforementioned lemmas, for all X, Y in the groups, we can reach Y from X through $X \to A \to Y$, where A is an element of the generating set. ■

Problem 6:
(a) Make a list H of all permutations in S_4 that can be written as products of permutations (123) and (234) (possibly with many factors in arbitrary order).
(b) Prove that H is a subgroup of S_4 and that $\{(123),(234)\}$ is its generating set.
(c) Draw the Cayley graph of H using the generating set found in part (b) in such a way that the arrows do not intersect.

Solution. (a) $H = \{Id, (123), (234), (12)(34), (13)(24), (132), (243), (142), (124), (143), (134), (14)(23)\}$, for a total of 12 permutations.

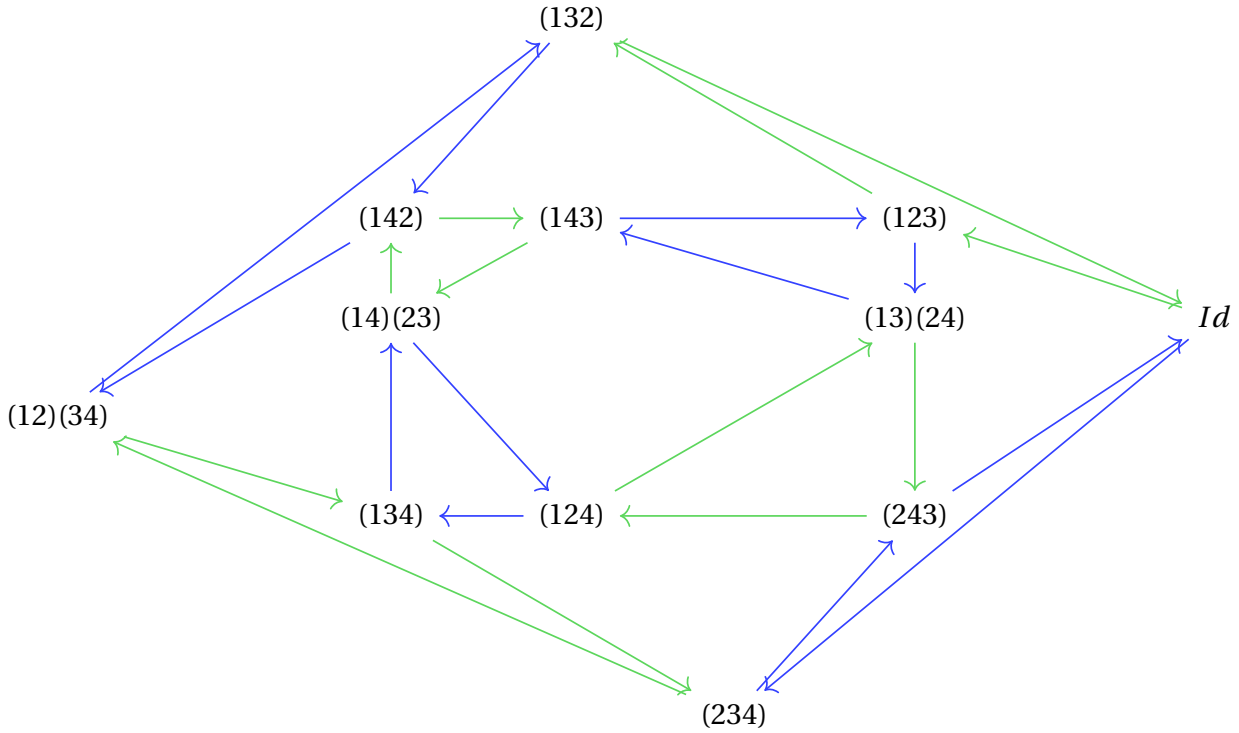
(b)

(1) First, we notice that H is non-empty. $H \subset S_4$, and the operation of H and S_4 are both composition.

(2) Second, for all $A, B \in H$, since A can be written as the products of permutations (123), (234), and so does B, $A \cdot B$ can be written as the composition of the products of (123), (234), which is also a product (123)'s and (234)'s. So H is closed with operation.

(3) Third, for all elements $A \in H$, we can determine A^{-1} by writing the inverse of the permutations in A in the reversed order.
For instance, if $A = R \cdot S$, then $A^{-1} = S^{-1} \cdot R^{-1}$. So H is closed with the inverse.

So H is a subgroup of S_4 by the Subgroup Test. Because from (a), we know that all elements of H is generated by $\{(123),(234)\}$, this is the generating set of subgroup H
(c) Let the blue arrows denote the operation with (234) and the green arrows denote the operations with (123). Then the Cayley graph will be:



■

Problem 7: For each of the following groups, describe all possible subgroups and prove that you have found all of them:
(a)$\mathbb{Z}_7$; (b) $\mathbb{Z}_7^*$; (c) D_3.

Solution. We will prove the following theorem:

Theorem 1 (Lagrange's Theorem)**.** *For every group G and its subgroup H, $|G| = n|H|$ for some positive integer n.*

Proof. For $r \in G$, denote Hr to be the set of all elements $x \cdot r, x \in H$. Then, we can conclude that: $Hr = Hs \iff s \in Hr \wedge r \in Hs$. In fact,

(1) $s \in Hs$ since H contains the identity element. Thus, $Hr = Hs \implies s \in Hr$.

(2) $s \in Hr \implies s = h_1 r$, for some $h_1 \in H$. Thus, $hs = hh_1 r, \forall h \in H$. and since $hh_1 r \in Hr \implies hs \in Hr \forall h \in H$, and $|Hs| = |Hr|$, we can conclude that $Hs = Hr$

Return to the proof, we select an element r_1. Then $|Hr_1| = |H| \leq |G|$. If $|H| = |G|$ then the theorem is proven, otherwise, there exists $r_2 \notin Hr_1$. So $Hr_2 \neq Hr_1$ By the observation above, Hr_1 and Hr_2 are disjoint. Otherwise, they must share a common element c such that $Hr_1 = Hg = Hr_2$, a contradiction. Continuing the process, we can partition G into n separate groups $Hr_1, Hr_2, \cdots, Hr_n$. ■

After listing the possible subgroups we will use Theorem 1 to prove that we have found all of them.

(1) Because $|\mathbb{Z}_7| = 7$, then a subgroup H may only have either $|H| = 1$ $|H| = 7$.
If $|H| = 1$,, then it must contain the identity element 0, so $|H| = \{0\}$. Else, $|H| = \mathbb{Z}_7$

(2) Because $|\mathbb{Z}_7^*| = 6$, then a subgroup H may have $1, 2, 3,$ or 6 elements.

- If $|H| = 1$, then similar to part (a), H contains the identity element, so $H = \{1\}$
- If $|H| = 2$, then H must also contain an identity element and another element whose inverse is itself. The only element with such property in $\mathbb{Z}_7^*$ is 6, so $H = \{1, 6\}$
- If $|H| = 3$, then H must contain $1, a, b$, where either $ab = ba = 1$, or $aa = bb = 1$. But since we know from the previous case there is only one element $a = 6$ such that $aa = 1 \mod 7$, a, b must be inverses of each other. So $H \in \{\{1, 2, 4\}, \{1, 3, 5\}\}$
- If $|H| = 6$, then $H = \mathbb{Z}_7^*$

In conclusion, $H \in \{\{1\}, \{1, 6\}, \{1, 2, 4\}, \{1, 3, 5\}, \{1, 2, 3, 4, 5, 6\}\}$

(3) Denote the rotation by 120 degrees counter-clockwise to be operation R, and the symmetry across one vertex and the center be S
Because $|D_3| = 6$, similar to part (b), a subgroup H may only have $1, 2, 3,$ or 6 elements.

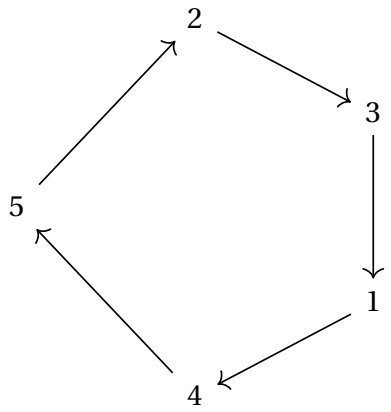
- If $|H| = 1$, then similar to part (a), H contains the identity element, so $H = \{Id\}$
- If $|H| = 2$, then H must also contain an identity element and another element whose inverse is itself, which can be: S, RS, R^2S. So $H \in \{\{Id, S\}, \{Id, RS\}, \{Id, R^2S\}\}$

- If $|H| = 3$, then H must contain $1, a, b$, where either $ab = ba = 1$, or $aa = bb = 1$. If a, b are inverses of each other, then they must be R and R^2. Otherwise, if a, b are inverses of themselves, they can be any 2-combination of $\{S, RS, R^2S\}$. So $H \in \{\{Id, R, R^2\}, \{Id, S, RS\}, \{Id, S, R^2S\}, \{Id, RS, R^2S\}\}$
- If $|H| = 6$, then $H = D_3$ In conclusion, $H \in \{\{Id\}, \{Id, S\}, \{Id, RS\}, \{Id, R^2S\}, \{Id, R, R^2\}, \{Id, S, RS\}, \{Id, S, R^2S\}, \{Id, RS, R^2S\}, D_3\}$

■

Problem 8: Compute the number of permutations in S_5 that are cycles. Prove that your computation is correct.

Solution. For every way to put five numbers on the circle, we can construct a cyclic permutation of S_5, by mapping each number to the number next to it in clockwise order. For instance,



will correspond to the cycle (14523). Vice versa, we can also construct a way to put 5 numbers on a circle for each cycle.
Assume that there are 2 cycles that correspond with the same circle. Then, by definition of the construction of the cycle, each of the numbers in both cycles must have the exact same mappings. Hence, the two cycles must be the same.

As a result, the number of permutations in S_5 that are cycles is equal to the number of ways to put 5 numbers onto a circle without rotation, which is:

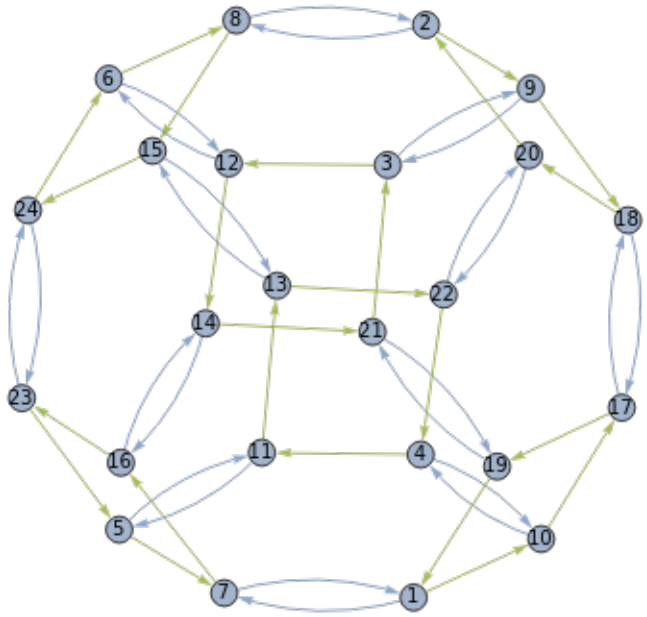
$$4! = 24 \text{ ways (permutations)}$$

■

Problem 9: Use Mathematica to draw the Cayley graph of the symmetric group S_4 using the following subsets as the generating sets: (a) {(12), (1234)}; (b) {(12), (23), (34)}

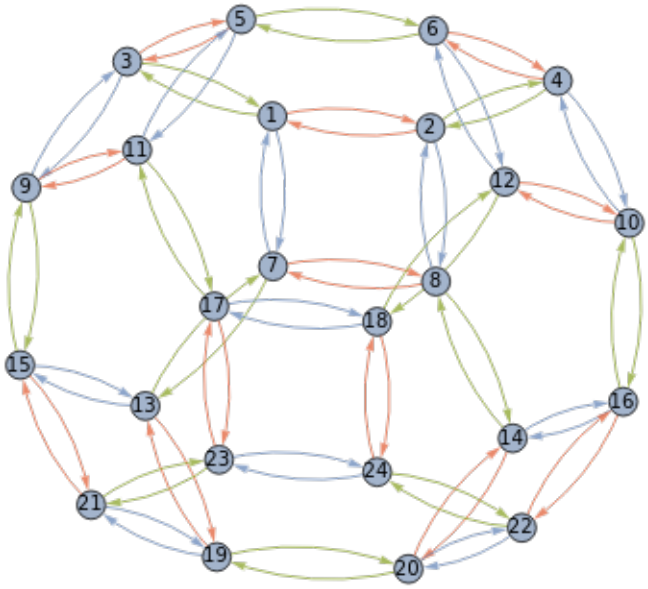
Solution. (a) The code for generating set {(12), (1234)}

```
CayleyGraph[PermutationGroup[{Cycles[{{1, 5, 4}}], Cycles[{{3, 4}}]}],
VertexLabels -> Placed["Name", Center], VertexSize -> 0.4]
```



(b) The code for generating set {(12), (23), (34)}

```
CayleyGraph[PermutationGroup[{Cycles[{{1,2}}], Cycles[{{2,3}}], Cycles[{{3,4}}]}],
VertexLabels -> Placed["Name", Center], VertexSize -> 0.4]
```



■