QUIZ TWO ANSWERS

1 Mandatory Section

1.1 Question 1

Let $G := \{M \in Mat_{2\times 2}(\mathbb{Z}/2\mathbb{Z}) | det(M) \equiv 1 \pmod 2\}$.
How many elements does this group have? What named group is G isomorphic to?

Answer: **6**, `SymmetricGroup(3)`
Enumerating elements of G:

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\}$$

This group is isomorphic to S_3.
To build the map it suffices to send generators of G to generators of S_3:

$$(1,2) \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } (1,2,3) \mapsto \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

1.2 Question 2

Consider the following cayley table of a group G:

$\times$	e	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
e	e	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
a	a	a^2	e	ab	ab^2	a^2b	b	a^2b^2	b^2
a^2	a^2	e	a	a^2b	a^2b^2	b	ab	b^2	ab^2
b	b	ab	a^2b	b^2	e	ab^2	a^2b^2	a	a^2
b^2	b^2	ab^2	a^2b^2	e	b	a	a^2	ab	a^2b
ab	ab	a^2b	b	ab^2	a	a^2b^2	b^2	a^2	e
a^2b	a^2b	b	ab	a^2b^2	a^2	b^2	ab^2	e	a
ab^2	ab^2	a^2b^2	b^2	a	ab	a^2	e	a^2b	b
a^2b^2	a^2b^2	b^2	ab^2	a^2	a^2b	e	a	b	ab

What is the smallest value of n such that G is isomorphic to a subgroup of S_n?

Answer: **6**
The order three elements a and b generate the abelian group G.
Consider the following identification: $a \mapsto (1,2,3)$ and $b \mapsto (4,5,6)$.
The identification can be built up to an isomorphism between G and the group generated by $(1,2,3)$ and $(4,5,6)$.

If n was smaller than 6, it would be impossible to find two elements of order three that commute.

2 Optional Section

2.1 Question 3

Let $\mathbb{X}$ be the set of all groups upto isomorphism.
Define an operation $Aut : \mathbb{X} \to \mathbb{X}$ as $G \mapsto Aut(G)$.
Consider the sequence:
$s := \{(\mathbb{Z}/26\mathbb{Z}), Aut(\mathbb{Z}/26\mathbb{Z}), Aut^{(2)}(\mathbb{Z}/26\mathbb{Z}), Aut^{(3)}(\mathbb{Z}/26\mathbb{Z}), \dots\}$

We call such a sequence *stationary* if there exists n such that $Aut^{(n+k)}(G) \simeq Aut^{(n)}(G)$ for all $k \in \mathbb{N}$ and we call $Aut^{(n)}(G)$ the stationary point.

What named group is the stationary point of s isomorphic to?
If you think s is not stationary, type : `NA`

Answer: `SymmetricGroup(3)`
Lemma: $Aut(\mathbb{Z}/n\mathbb{Z}) \simeq U(n)$
Using the lemma, we have $Aut(\mathbb{Z}/26\mathbb{Z}) \simeq U(26)$.
With SageMath, we can deduce $< 15 >= U(26)$, thus $U(26) \simeq (\mathbb{Z}/12\mathbb{Z})$.

Applying the lemma again, we have $Aut(\mathbb{Z}/12\mathbb{Z}) \simeq U(12)$.
Now $U(12) = \{1, 5, 7, 11\}$ and observe $5^2 \equiv 7^2 \equiv 1 \pmod{12}$.
$Aut(U(12))$ is isomorphic to the Klein Four group.

The automorphism group of Klein Four is not too difficult to determine.
The identity element must be mapped to itself and since all other elements have order 2 and are abelian, they can be mapped amongst each other in any order.
Thus the automorphism group is isomorphic to S_3.

Interestingly, $Aut(S_3) \simeq S_3$.
Lemma: Any two cycle together with any three cycle generate S_3.
Since isomorphisms preserve order, there are 3 ways to map the two cycle and 2 ways to map the three cycle - 6 isomorphisms in total.
Observe that the two maps $\phi_1(\sigma) = (1,2)\sigma(1,2)$ and $\phi_2(\sigma) = (1,3)\sigma(1,3)$ do not commute. Thus $Aut(S_3)$ is a non-abelian group of order 6.

Thus the sequence turns out to be $\{(\mathbb{Z}/26\mathbb{Z}), (\mathbb{Z}/12\mathbb{Z})$, Klein Four, $S_3, S_3, \dots\}$.
The stationary point is S_3.

Can you find a group G such that $\{G, Aut(G), Aut^{(2)}(G), Aut^{(3)}(G), \dots\}$ has no stationary point?

2.2 Question 4

How many subgroups of S_5 are isomorphic to the Klein Four group?

Answer: **20**
The Klein Four group has elements $\{e, a, b, ab\}$ where $a^2 = b^2 = e$ and $ab = ba$.

One way to identify this group is to pick a pair of disjoint two cycles:
The group generated by (a, b) and (c, d) where a, b, c, d are distinct values from $\{1, 2, 3, 4, 5\}$.
There are $\frac{\binom{5}{2}\binom{3}{2}}{2} = 15$ such groups.

Another way to identify this group as a permutation group comes from the cayley table:

$\times$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Observe that the last four entries in each row of the table is a permutation of the last four entries of the first row.
This sets up an identification $e \mapsto ()$, $a \mapsto (1, 2)(3, 4)$, $b \mapsto (1, 3)(2, 4)$ and $ab \mapsto (1, 4)(2, 3)$.
The choice of the numbers $\{1, 2, 3, 4\}$ was arbitrary, thus there are $\binom{5}{4} = 5$ such subgroups.

In total[1], there are 20 subgroups of S_5 that are isomorphic to the Klein Four group.

2.3 Question 5

Consider the rectangular '5-puzzle' as shown below:

1	2	3
4	5	B

The set of moves that keep the blank tile 'B' in the bottom right corner forms a group G under the composition operation. What is the cardinality of the minimal generating set of the group G?

Answer: **2**
Observe that the two moves `squareRot` and `rectangleRot` preserve the position of the blank tile.

[1] As an exercise, verify that this list is exhaustive.

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 & \mathrm{B} \\ \hline\end{array} \longrightarrow \begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 4 & 2 & \mathrm{B} \\ \hline\end{array}$$

`squareRot`

$$\begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 & \mathrm{B} \\ \hline\end{array} \longrightarrow \begin{array}{|c|c|c|}\hline 4 & 1 & 2 \\ \hline 5 & 3 & \mathrm{B} \\ \hline\end{array}$$

`rectangleRot`

We can encode `squareRot` as the permutation $(2, 3, 5)$ and `rectangleRot` as $(1, 2, 3, 5, 4)$.
With SageMath we get a candidate for the group G:

```
G = PermutationGroup([[(2,3,5)],[(1,2,3,5,4)]])
print(G.structure_description())
```

`Out : ‘A5’`

The set of all puzzle configurations is a subgroup of S_6, however since we are fixing the blank tile at the bottom right, this means that the group of configurations is a subgroup of S_5.
Thus the group can be either A_5 or S_5.

Observe that the state encoded by $(1, 2)$ cannot be reached without breaking the puzzle.
Since we impose the condition that the blank tile must remain in the same bottom right position, the number of up and down, right and left moves must be equal.
Observe each move up, down, right and left is a transposition, hence all reachable states must be encoded by even permutations.

We have stumbled into a generating set of the group G whose cardinality is 2.
We cannot have a generating set with a single set, as this would mean the group G is cyclic (which it is not).

If `squareRot` and `rectangleRot` were not identified, after deducing that G is isomorphic to A_5, we can use this snippet:

```
print(len(AlternatingGroup(5).gens_small()))
```

`Out : ‘2’`

2.4 Question 6

Let G be a group generated by two elements x and y (and their symbolic inverses x^{-1} and y^{-1}) such that $xyx^{-1} = y^2$ and $y^{-1}xy = x^2$.
What is the order of the group G?
If you think the group's order cannot be computed, type :`NA`

Answer: **1**
G is isomorphic to the the trivial group.
From the second relation we have $xy = (yx)x$.
Plugging this into the first relation, we get $(yx)(xx^{-1}) = y^2$.
Thus $yx = y^2$ and by the cancellation law, we get $x = y$.
The group can be generated with just one generator!

Plugging this back in the second relation, we get $x^{-1}xx = x^2$.
Thus $x = x^2$.
Lemma: The only idempotent in a group is the identity element.[2]

Thus G is the group generated by $\{e, e\}$ - the trivial group.[3]

[2]A direct consequence of the cancellation law.
[3]This was an easy instance of the undecidable group isomorphism decision problem