A few general remarks about homeworks.

I’m not very happy when I see an answer with no explanation. A good explanation can give substantial partial credit when the answer has a glitch. I can also help you understand better when I know what you are thinking.

As I’ve said, I encourage you to work together on the homework, but please check your work before you submit it. It’s awkward for me to see the identical silly typo in several papers!

On HW 1, I will weight problem 5 less, but usually all problems have equal weight.
Just some quick review. Suppose you have a group \((G, \ast)\) and its multiplication table. For any \(x \in G\), you can write down the powers from only looking at the table \(x^2 = x \ast x, x^3 = x \ast (x^2)\).

In some cases, you are lucky and find that \(e, x, x^2, \ldots, x^{m-1}\) are distinct and are the elements of \(G\) in some order and that \(x^m = e\). In this case, \((G, \ast)\) is a cyclic group of order \(m\).

So, for example, you showed in HW1 that \(((\mathbb{Z}/14\mathbb{Z})^*, \circ)\) is a cyclic group of order 6 with generators \([3]_{14}\) or \([5]_{14}\). You can work out the powers just from looking at the table. You don’t have to calculate \(5^5\) and reduce it mod 14.
Look at the powers: $5^2 = 5 \times 5 = 11$, $5^3 = 5 \times 5^2 = 5 \times 11 = 13$, $5^4 = 5 \times 5^3 = 5 \times 13 = 9$, $5^5 = 5 \times 5^4 = 5 \times 9 = 3$, $5^6 = 5 \times 3 = 1$.

Also, $11^2 = 11 \times 11 = 9$, $11^3 = 11 \times 11^2 = 9 \times 11 = 1$, so $\langle [11]_{14} \rangle$ is a cyclic subgroup of order 3.

For fun, notice that $13 \equiv -1 \mod 14$, 

<table>
<thead>
<tr>
<th>$(\mathbb{Z}/14\mathbb{Z})^*$</th>
<th>1</th>
<th>3</th>
<th>5</th>
<th>9</th>
<th>11</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>9</td>
<td>11</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>13</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>1</td>
<td>11</td>
<td>3</td>
<td>13</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>13</td>
<td>3</td>
<td>11</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>5</td>
<td>13</td>
<td>1</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>11</td>
<td>9</td>
<td>15</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>
How do you make an isomorphism from a $G = \langle x \rangle$ that is cyclic with order $m$ and generator $x$ with the more familiar $C_m = \langle a \rangle$? It is very easy: define $\Phi$ so that

$$\Phi(a^k) = x^k.$$  

Then $\Phi(a^k \cdot a^j) = \Phi(a^{k+j}) = x^{k+j} = x^k \cdot x^j$, $\Phi(a^m) = x^m = e$, etc. So to give an isomorphism from $C_6$ to $((\mathbb{Z}/14\mathbb{Z})^*, \circ)$, one is

$$\Phi(e) = [1]_{14},$$
$$\Phi(a) = [3]_{14},$$
$$\Phi(a^2) = [3^2]_{14} = [9]_{14},$$
$$\Phi(a^3) = [3^3]_{14} = [9 \cdot 3]_{14} = [13]_{14},$$
$$\Phi(a^4) = [3^4]_{14} = [13 \cdot 3]_{14} = [11]_{14},$$
$$\Phi(a^5) = [3^5]_{14} = [11 \cdot 3]_{14} = [5]_{14}.$$  

You could give a second isomorphism $\Phi'$ by $\Phi'(a) = [5]_{14}$, because $(\mathbb{Z}/14\mathbb{Z})^* = \langle [3]_{14} \rangle = \langle [5]_{14} \rangle$. Any generator will do.
How do you check that a subset $H$ of a group $(G, \ast)$ is a subgroup? You check that it is closed under $\ast$, that it contains the identity and that it contains the inverses of every element in it.

One type of subgroup works for every group $(G, \ast)$. For $x \in G$ take $\langle x \rangle$. This will always be closed under $\ast$, it has the identity and inverses.

When $G$ is a cyclic group, this is the only possible kind of subgroup: The subgroups of $C_n$ are $\langle x^k \rangle$, where $k$ divides $n$.

It is possible for $G$ to be not a cyclic group and this is true for proper subgroups too: take $V$ or $S_3$.

I think we already saw that the only subgroups of $V$ are

$$\{e\}, \{e, X\}, \{e, Y\}, \{e, Z\}, \{e, X, Y, Z\}$$
Here’s the multiplication table for $S_3$

<table>
<thead>
<tr>
<th>$S_3$</th>
<th>$\rho_0$</th>
<th>$\rho_1$</th>
<th>$\rho_2$</th>
<th>$\mu_1$</th>
<th>$\mu_2$</th>
<th>$\mu_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rho_0$</td>
<td>$\rho_0$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
<td>$\mu_3$</td>
</tr>
<tr>
<td>$\rho_1$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
<td>$\rho_0$</td>
<td>$\mu_3$</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
</tr>
<tr>
<td>$\rho_2$</td>
<td>$\rho_2$</td>
<td>$\rho_0$</td>
<td>$\rho_1$</td>
<td>$\mu_2$</td>
<td>$\mu_3$</td>
<td>$\mu_1$</td>
</tr>
<tr>
<td>$\mu_1$</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
<td>$\mu_3$</td>
<td>$\rho_0$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
</tr>
<tr>
<td>$\mu_2$</td>
<td>$\mu_2$</td>
<td>$\mu_3$</td>
<td>$\mu_1$</td>
<td>$\rho_2$</td>
<td>$\rho_0$</td>
<td>$\rho_1$</td>
</tr>
<tr>
<td>$\mu_3$</td>
<td>$\mu_3$</td>
<td>$\mu_1$</td>
<td>$\mu_2$</td>
<td>$\rho_1$</td>
<td>$\rho_2$</td>
<td>$\rho_0$</td>
</tr>
</tbody>
</table>

Let’s find all the subgroups of $S_3$.

The identity $\rho_0$ is in every subgroup. Suppose $H$ is a subgroup of $G$ and $\rho_1 \in H$. Then $\rho_1 \circ \rho_1 = \rho_2 \in H$ and since $\rho_1^3 = \rho_0$, $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ is a subgroup of $S_3$.

You can also check that $\langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}$. Suppose $H$ is a subgroup that contains $\rho_2$. The same argument shows that $H$ contains $\{\rho_0, \rho_1, \rho_2\}$.
Now suppose a subgroup $H$ contains all the $\rho_j$’s and one of the $\mu_i$’s. One look at the multiplication table shows that you get the other two $\mu_i$’s as well, so $H = S_3$.

So any other subgroup cannot have $\rho_1$ or $\rho_2$. If it has one $\mu_j$, since $\mu_j \circ \mu_j = \rho_0$, we have the three subgroups $\langle \mu_j \rangle = \{\rho_0, \mu_j\}$.

Suppose a subgroup $H$ has two different $\mu_j$’s, say $\mu_j$ and $\mu_k$. Then it has $\mu_j \circ \mu_k$, which will be $\rho_1$ or $\rho_2$, so we get all of $S_3$.

This gets harder as the groups get larger.
WORKSHEET PROBLEM

1. Suppose $\alpha$ and $\beta$ are two permutations in $S_5$ given by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} = (1243)(5), \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix},$$

a. Write $\beta$ in cycle form.

b. Compute $\alpha \circ \beta$. (Remember that $(\alpha \circ \beta)(i) = \alpha(\beta(i))$.)
WORKSHEET PROBLEM SOLUTION

For reference:

\[ \alpha = \begin{pmatrix} 12345 \\ 24135 \end{pmatrix}, \quad \beta = \begin{pmatrix} 12345 \\ 35124 \end{pmatrix}, \]

a. So \( \alpha = (1243)(5) \) and \( \beta = (13)(254) \) and \( \alpha(\beta(i)) \) is given by

\[
\begin{align*}
\alpha(1) &= 2 & \beta(1) &= 3 & \Rightarrow & & (\alpha \circ \beta)(1) &= \alpha(3) = 1 \\
\alpha(2) &= 4 & \beta(2) &= 5 & \Rightarrow & & (\alpha \circ \beta)(2) &= \alpha(5) = 5 \\
\alpha(3) &= 1 & \beta(3) &= 1 & \Rightarrow & & (\alpha \circ \beta)(3) &= \alpha(1) = 2 \\
\alpha(4) &= 3 & \beta(4) &= 2 & \Rightarrow & & (\alpha \circ \beta)(4) &= \alpha(2) = 4 \\
\alpha(5) &= 5 & \beta(5) &= 4 & \Rightarrow & & (\alpha \circ \beta)(5) &= \alpha(4) = 3.
\end{align*}
\]

So

\[ \alpha \circ \beta = \begin{pmatrix} 12345 \\ 15243 \end{pmatrix} = (1)(253)(4). \]
Have a good and safe weekend!