GSI: Seewoo Lee.

1. There are **10** subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_6$. Here is a complete list of them, in increasing order of size:

$$
\begin{aligned}
\langle(0,0)\rangle &= \{(0,0)\} \\
\langle(1,0)\rangle &= \{(0,0),(1,0)\} = \mathbb{Z}_2 \times \{0\} \\
\langle(0,3)\rangle &= \{(0,0),(0,3)\} = \{0\} \times \langle 3\rangle \\
\langle(1,3)\rangle &= \{(0,0),(1,3)\} \\
\langle(0,2)\rangle &= \{(0,0),(0,2),(0,4)\} = \{0\} \times \langle 2\rangle \\
\langle(1,0),(0,3)\rangle &= \{(0,0),(1,0),(0,3),(1,3)\} = \mathbb{Z}_2 \times \langle 3\rangle \\
\langle(1,2)\rangle &= \{(0,0),(1,2),(0,4),(1,0),(0,2),(1,4)\} = \mathbb{Z}_2 \times \langle 2\rangle \\
\langle(0,1)\rangle &= \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5)\} = \{0\} \times \mathbb{Z}_6 \\
\langle(1,1)\rangle &= \{(0,0),(1,1),(0,2),(1,3),(0,4),(1,5)\} \\
\langle(1,0),(0,1)\rangle &= \{(0,0),(1,0),(0,1),(1,1),(0,2),(1,2),(0,3),(1,3),(0,4),(1,4),(0,5),(1,5)\} = \mathbb{Z}_2 \times \mathbb{Z}_6
\end{aligned}
$$

   To show that these are all the subgroups, one way is to use Lagrange's theorem. Since the order of $\mathbb{Z}_2 \times \mathbb{Z}_6$ is 12, the order of any subgroup must divide 12, hence the order of any subgroup must be one of $1, 2, 3, 4, 6, 12$. Then, we can check that there are no other subgroups of each order. For example, when $d = 2, 3, 6$, all the abelian groups of order d are cyclic, so one only needs to find an element of order d to generate a subgroup of order d. When $d = 4$, there are two abelian groups of order 4 up to isomorphism, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$, and you need to check both cases. Note that not all of them are of the form $H_1 \times H_2$ for some $H_1 \le \mathbb{Z}_2$ and $H_2 \le \mathbb{Z}_6$; $\langle(1,3)\rangle$ and $\langle(1,1)\rangle$ are counterexamples. (If you still don't believe me, type `AllSubgroups(DirectProduct(CyclicGroup(2),CyclicGroup(6)));` in this website which gives you a list of length 10, not in a form you expected though.)

   I find that it is not an easy problem to enumerate all the subgroups of a given finite abelian group, even if we know all of them *up to isomorphism* (FTFGAG). For the interested reader, see here.

2. Here is a more detailed explanation of why the Cayley graph in #2 cannot be a Cayley graph of the quaternion group Q. There are two generators shown in the graph, one of which has order 4 (the one that goes around the square) and the other has order 2 (the one that goes across the square). Let the generators be a and b. The only element of order 2 in Q is $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, so b must be that. The other six elements (besides the identity) have order 4, so a can be any of them. However, we have $a^2 = b$ for all of them, which means that $\{a, b\}$ never generates Q.

   Also, one correction for the section is that there are **5** elements of D_4 of order 2: the four reflections and the 180° rotation.

3. Here is a sketch of a proof (as an exercise) that S_n is generated by two elements $(1,2)$ and $(1,2,\dots,n)$. One general tip for doing mathematics is to keep reducing the problem to simpler ones until you reach something you already know how to do.

   (a) For any $a, b, c \in \{1, 2, \dots, n\}$, show that $(a\,b)(a\,c)(a\,b) = (b\,c)$. Deduce that any transposition can be written as a product of $(1\,2), (1\,3), \dots, (1\,n)$.

   (b) Show that $(1\,k)$ can be written as a product of $(1\,2)$ and $(1\,2\,\dots,n)$ for $k = 3, 4, \dots, n$. To do this, think about the product

$$(1\,2\,\dots\,n)^{-m}(1\,2)(1\,2\,\dots\,n)^m$$

   for $m \ge 1$. Then this permutation has order 2 - why? What is it?

   In general, the map sending $g \in G$ to $hgh^{-1} \in G$ for some $h \in G$ is called **conjugation by** h, which is *extremely* important in group theory. You have probably seen conjugation in linear algebra as a change of basis.