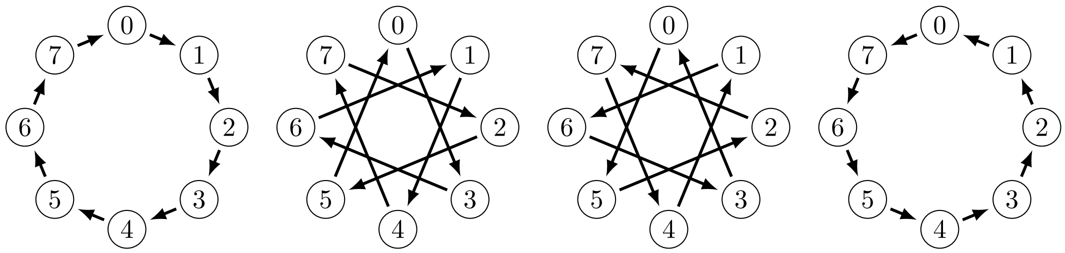
GSI: Seewoo Lee.

1. (a) In general, a is a generator of $\mathbb{Z}_n$ if and only if $\gcd(a,n)=1$. So the generators of $\mathbb{Z}_8$ are $1,3,5,7$.

   (b) Here are the Cayley graphs of $\mathbb{Z}_8$ with respect to the generating sets $\{1\},\{3\},\{5\},\{7\}$, respectively.

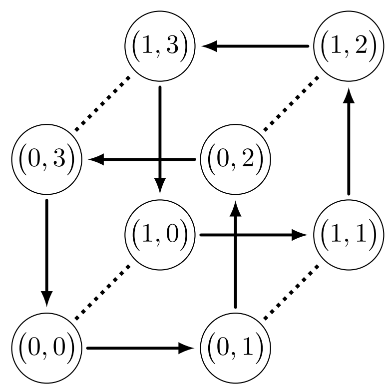


   Note that all four graphs are isomorphic to each other; you can "untangle" the second and third graphs to look like the first one. This reflects the fact that, for any pair $(\mathbb{Z}_8, S_1)$ and $(\mathbb{Z}_8, S_2)$ where S_1 and S_2 are generating sets of size 1, there exists an automorphism of $\mathbb{Z}_8$ that sends S_1 to S_2.

2. (a) $2\times 4 = 8$.

   (b) It is not cyclic. If (a,b) is a generator of the group, then it should have order 8. However, the order of any element is at most 4, since $(a,b)^4 = (4a,4b) = (0,0)$ (identity).

   (c) There can be many choices, but you need at least two elements since the group is not cyclic. For example, $S=\{(1,0),(0,1)\}$ is a generating set. The corresponding Cayley graph is as follows:

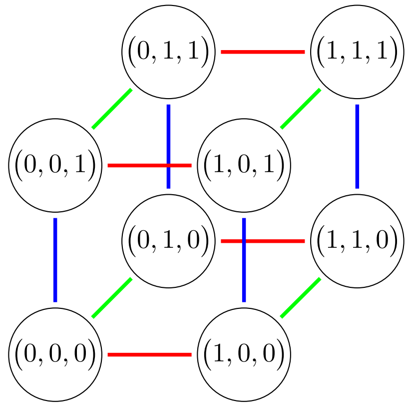


   Here the solid arrows (resp. dotted edges) correspond to adding $(0,1)$ (resp. $(1,0)$).

3. Here's a cube with vertices labeled by coordinates, with three colors (red, green, and blue): Note that the group you get here is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, where each color corresponds to adding $(1,0,0)$, $(0,1,0)$, $(0,0,1)$.

   (a) You need to check that (1) the graph is connected, (2) there is at most one edge between any two vertices, (3) each vertex g has exactly one arc of each color starting at g, and (4) if two different sequences of arc types starting from g end at the same vertex h, then the same sequences starting from any vertex u also end at the same vertex. It is easy to see that (1), (2), and (3) hold. To "show" (4), one can observe that following an edge of a specific color corresponds to flipping a specific coordinate of vertices, and the final vertex only depends on which coordinates are flipped, not the order of flipping.

   (b) Yes. It is enough to check that the generators commute. (Why?) We can check this by following the paths in the Cayley graph that correspond to ab and ba for two generators a,b, and see that they end up at the same vertex.



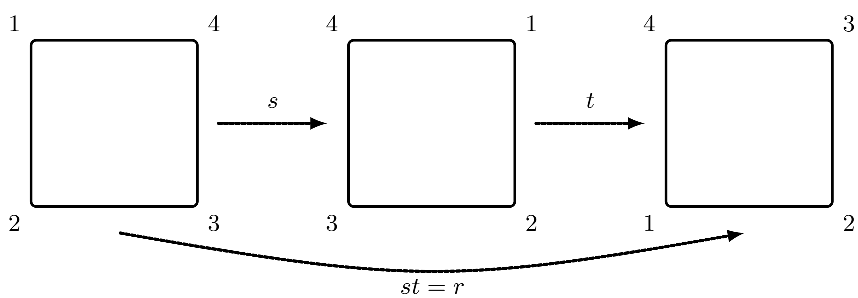
(c) Since all edges are bidirectional, the generators are of order 2. (a^2 corresponds to following an edge forward then backward.) Since the group is abelian, all other elements are also of order at most 2. (Why?)

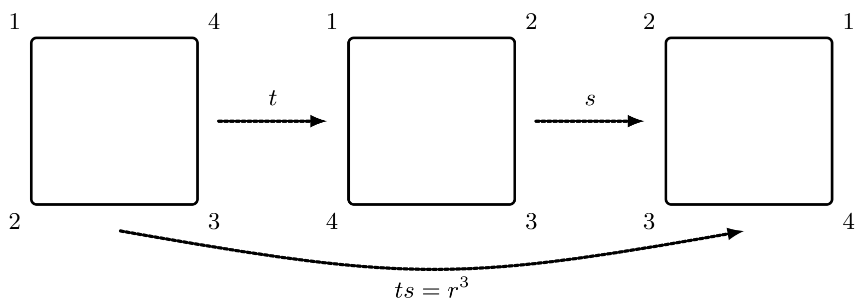
4. (a) There are 8 symmetries: 4 rotations (including the identity) and 4 reflections (horizontal, vertical, and two diagonals).

(b) $\{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. The last four elements are reflections (identify which ones).

(c) The figures below show that $st = r$ and $ts = r^3 = (st)^3$.[1] Using these relations with $s^2 = t^2 = e$ (since s and t are reflections), one can rewrite the elements in (b) in terms of s and t as follows:

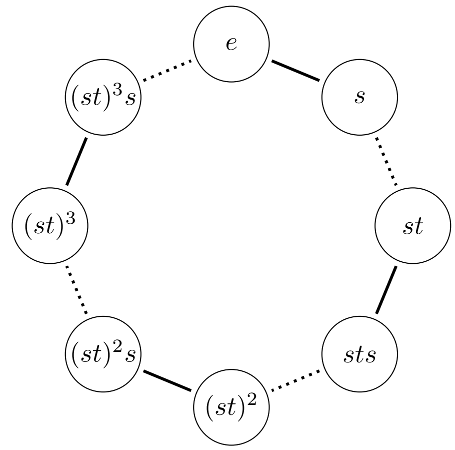
$$e = e, \quad r = st, \quad r^2 = (st)^2, \quad r^3 = (st)^3,$$
$$s = s, \quad sr = t, \quad sr^2 = tst, \quad sr^3 = tstst.$$





(d) Here is a Cayley graph of D_4 with respect to the generating set $\{s, t\}$. The solid edges correspond to s and the dotted edges correspond to t.

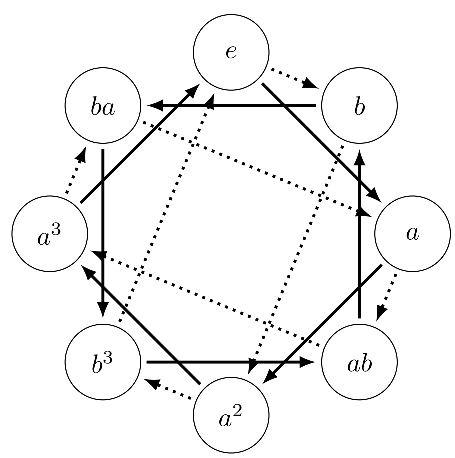
[1] Here the symmetries are applied from left to right, i.e., st means first applying s, then applying t. In other words, the group *acts on the square from the right.*



5. (a) A brute-force way to check closure is to multiply every pair of matrices and see that the result is still in Q.
   (b) The only matrix of order 2 is $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$. The remaining six matrices (besides the identity) have order 4—all of their squares are $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$.
   (c) We can express all 8 matrices in terms of a and b as follows:

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = e, \quad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = a, \quad \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} = ba = a^3b, \quad \begin{pmatrix}0 & i\\ i & 0\end{pmatrix} = b,$$
$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = a^2, \quad \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = a^3, \quad \begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix} = ab = b^3a, \quad \begin{pmatrix}0 & -i\\ -i & 0\end{pmatrix} = b^3 = a^2b.$$

   The corresponding Cayley graph is as follows:



6. To distinguish the above groups, we can use certain structural properties of groups. For example, being an abelian group is a structural property, and it shows that the first three groups are different from the last two groups. To distinguish the first three groups, we can distinguish the first group from the other two groups by checking whether a group is cyclic or not. For the second and third groups, all the elements of the third group are of order at most 2, while the second group has an element of order 4 (*having an element of order 4* is also a structural property). To distinguish D_4 and Q, we can check the number of elements of order 2. D_4 has 5 elements of order 2 (r^2 and the four reflections), while Q has only one element of order 2.

   Showing that any group of order 8 is isomorphic to one of the above groups is harder. I don't even know if it is possible to do this without using theorems that we haven't learned yet (let me know if you find a way!). See pages 2–4 of this note for a proof. Prerequisites for the proof are Lagrange's theorem and cosets (so you may be able to understand the proof before the midterm).

Note that Cayley graphs might not be useful to distinguish groups, since Cayley graphs depend on the choice of generating sets. In particular, two isomorphic groups can have non-isomorphic Cayley graphs if you choose different generating sets. Having isomorphic Cayley graphs tells you more than being isomorphic as groups; if (G_1, S_1) and (G_2, S_2) have isomorphic Cayley graphs, then there exists an isomorphism from G_1 to G_2 *that sends* S_1 *to* S_2.