Problem Set 12

Exercise 1:
Consider the matrices

\[
I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad C = AB
\]

by definition, so \( C = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \)

in \( M_2(\mathbb{C}) \). Direct matrix calculations show that \( AB = C, \ BC = A, \ CA = B \) and \( A^2 = B^2 = C^2 = -I \).

1. Using ONLY the algebraic identities above prove that these matrices have the additional "commutation relations"

\[
BA = -AB = -C, \ CB = -BC = -A, \ AC = -CA = -B
\]

\[
A^{-1} = -A, \ B^{-1} = -B, \ C^{-1} = -C
\]

Note: A proof by direct matrix calculations will not be accepted. The point here is to see if you can derive new algebraic relations from those already known above.

2. Prove that the multiplicative matrix group generated by \( A, B, C \) is precisely the set of eight matrices \( Q_8 = \{ \pm I, \pm A, \pm B, \pm C \} \).

3. Fill in all entries of the following multiplication table for the group \( Q_8 \).
4. Determine the center $Z(Q_8)$.

5. Describe all conjugacy classes in this group. (If you have got them all the class equation should be satisfied.)

**Solution:**

1. $AB = C$ and $A^2 = -I$ implies $BA = -A^2BA = (-I)A(AB)A = -IA \cdot C \cdot A = -A \cdot B = -C$. By similar reasoning $CB = -B^2CB = -A$ and $AC = -C^2AC = -B$. The identities $A^{-1} = -A, \ldots, C^{-1} = -C$ follow because $A^2 = -I$ implies $(-A)A = I$ implies $-A = A^{-1}$, etc.

2. $Q_8$ contains the cyclic groups $<A> = \{I, A, -I, A\}$, $<B> = \{\pm I, \pm B\}$, $<C> = \{\pm I, \pm A, \pm B, \pm C\}$. To get equality it suffices to show this set of 8 elements is a group. Obviously, $I$ acts as an identity. It suffices to prove pairwise products of $A, B, C$ are in $Q_8$ since then $-I \in Q_8$ then their negatives are also in $Q_8$ as are $A^2 = B^2 = C^2 = -I$.

That leaves just 3 products $BA, CB, AC$ to examine. But by 1.

$$BA = -AB = -C, \ CB = -BC = -A, \ AC = -CA = -B$$

are all in $Q_8$, so all products are in $Q_8$.

As for inverses $A^2 = -I$ then $(-A)A = I$ then $A^{-1} = -A$ and similarly $B^{-1}, C^{-1} \in Q_8$. Then $(-B)^{-1} = (-I)B^{-1} = B \in Q_8$ and likewise $(-A)^{-1}, (-C)^{-1}$ are in $Q_8$.

Since $(-I)^{-1} = -I$, all elements in our list have inverses in the list.

Finally, matrix multiply is associative so $Q_8$ is a group of matrices under multiplication.

3. 

<table>
<thead>
<tr>
<th></th>
<th>I</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>I</th>
<th>-A</th>
<th>-B</th>
<th>-C</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>I</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>-I</td>
<td>-A</td>
<td>-B</td>
<td>-C</td>
</tr>
<tr>
<td>A</td>
<td>A</td>
<td>-I</td>
<td>C</td>
<td>-B</td>
<td>-A</td>
<td>I</td>
<td>-C</td>
<td>B</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
<td>-C</td>
<td>-I</td>
<td>A</td>
<td>-B</td>
<td>C</td>
<td>I</td>
<td>A</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>B</td>
<td>-A</td>
<td>-I</td>
<td>-C</td>
<td>-B</td>
<td>A</td>
<td>I</td>
</tr>
<tr>
<td>-I</td>
<td>-I</td>
<td>-A</td>
<td>-B</td>
<td>-C</td>
<td>I</td>
<td>A</td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td>-A</td>
<td>-A</td>
<td>I</td>
<td>-C</td>
<td>B</td>
<td>A</td>
<td>-I</td>
<td>C</td>
<td>-B</td>
</tr>
<tr>
<td>-B</td>
<td>-B</td>
<td>C</td>
<td>I</td>
<td>-A</td>
<td>B</td>
<td>-C</td>
<td>-I</td>
<td>A</td>
</tr>
<tr>
<td>-C</td>
<td>-C</td>
<td>-B</td>
<td>A</td>
<td>I</td>
<td>C</td>
<td>B</td>
<td>-A</td>
<td>-I</td>
</tr>
</tbody>
</table>
4. $\mathbb{Z}(\mathbb{Q}_8) = \{I, -I\} \simeq \mathbb{Z}/2\mathbb{Z}$. This can be seen by inspection the multiplication table, but can be seen directly. From 1., $AB \neq BA$, $BC \neq CB$, $CA \neq AC$ thus $A, B, C \notin Z(\mathbb{Q}_8)$ and then $-A, -B, -C \notin Z(\mathbb{Q}_8)$. On the other hand, in $M_2(\mathbb{C})$, the matrices $I, -I$ commute with everybody.

5. The one-point conjugacy are $C_1 = \{I\}$, $C_{-1} = \{-I\}$. Now consider the non trivial conjugate of $A : AAA^{-1} = A$, $BAB^{-1} = BA(-B) = -B(AB) = -BC = -A$ and similarly $CAC^{-1} = -CAC = -BC = -A$. Conjugation by $\pm I$ has us effect on $A$, and conjugation by $-A$, $-B$, $-C$ has some effect as conjugation by $A, B, C$. Hence $C_A = \{XAX^{-1} : X \in \mathbb{Q}_8\} = \{A, -A\}$. Similar calculations yield $C_B = \{B, -B\}$ and $C_C = \{C, -C\}$. All elements in $\mathbb{Q}_8$ are accounted for. (Note: The union of the one-point classes in $\{+I, -I\}$ as in 4.. Furthermore $|Z(G)| + |C_A| + |C_B| + |C_C| = 2 + 2 + 2 + 2 = 8 = |\mathbb{Q}_8|$ as expected.

Exercise 2:

The orthogonal group $G = O(n)$ is the group of matrices.

$$\{A \in M_n(\mathbb{R}) : A^tA = I = AA^t\} = \{A : A^t = A^{-1}\}$$

The special orthogonal group is the subgroup $H = SO(n) = \{A \in O(n) : \det(A) = +1\}$.

1. Verify that $G$ and $H$ are both groups.
2. Prove that $H$ is normal subgroup of $G$.
3. Prove that there are exactly two cosets in $G/H$, and that $G/H \simeq (\mathbb{Z}/2\mathbb{Z}, +)$.
4. Is $G$ isomorphic to a direct product of $SO(n)$ and $\mathbb{Z}/2\mathbb{Z}$? Is $G$ a semi direct product of $SO(n)$ and $\mathbb{Z}/2\mathbb{Z}$? Explain.

Solution:

1. If $A, B \in O(n)$ then $(AB)^tAB = B^t(A^tA)B = B^tIB = B^tB = I$ and similarly $(AB)(AB)^t = I$; thus $O(n)$ is closed under matrix product. The matrix $I \in O(n)$ obviously acts as a unit : $IA = A = AI$ for all $n \times n$ matrices. Finally; $A \in O(n)$ implies $A^t = A^{-1}$. Then $(A^{-1})^tA^{-1} = (A^t)^{-1}A^{-1} = (AA^t)^{-1} = I$ and similarly $(A^{-1})(A^{-1})^t = I$. Therefore $A^{-1} \in O(n)$. Thus $O(n)$ is a group. The map $\det : O(n) \rightarrow \mathbb{C}$ satisfies $\det(AB) = \det(A) \cdot \det(B)$. Obviously $\det(A^{-1}) = 1/\det(A)$ for any matrix with nonzero determinant since $AA^{-1} = I$ implies $\det(A)\det(A^{-1}) = \det(I) = 1$. Thus if $A, B \in O(n)$ have determinant equal to $\pm 1$. So do $AB$ and $A^{-1}$. $SO(n) = \{A \in O(n) : \det(A) = \pm 1\}$ is a subgroup of $O(n)$ too.

2. If $A \in O(n)$, then $A^tA = I$ . But $\det(A^t) = \det(A)$, hence $1 = \det(A^t) = \det(A^t)\det(A) = \det(A)^2$. Also $\det(A)$ is real since $A$ has real entries. The only $\lambda$ in $\mathbb{R}$ such that $\lambda^2 = 1$ are $\lambda = \pm 1$.

Since $\det : O(n) \rightarrow (\{\pm 1\}, \cdot) \simeq \mathbb{Z}/2\mathbb{Z}$ is a homomorphism, and $\det = 1$ on $SO(n)$, there can be at most two cosets of $H = SO(n)$ in $G = O(n)$. But in fact, there always exist $A \in O(n)$ at $\det(A) = -1$, for instance the matrix

$$\begin{pmatrix}
-1 & 0 \\
0 & 1 \\
0 & . \\
. & . \\
. & 1
\end{pmatrix}$$
Thus \( \ker(\det) = \SO(n) \), and \( \SO(n) \leq \O(n) \); there is one other coset in \( G/H \), given by \( R \cdot \SO(n) \) where \( R \) is any matrix in \( \O(n) \) such that \( \det(R) = -1 \).

3. We have already proved \( H = \SO(n) \) is normal in \( G = \O(n) \). Now consider the diagram

\[
\begin{array}{ccc}
G = \O(n) & \xrightarrow{\det} & K = \langle \{\pm 1\}, \cdot \rangle = \mathbb{Z}/2\mathbb{Z} \\
\downarrow \pi & \quad & \quad \downarrow \det^2 \\
G/H & \quad & \quad \\
\end{array}
\]

where \( \pi : G \to G/H \) is the quotient map, and apply the First isomorphism Theorem. Here \( K = \{\pm 1\} \) under multiplication as the group operation. The homomorphism \( \det : G \to K \) is surjective, and its kernel is precisely \( \ker(\det) = \langle A : \det(A) = +1 \rangle = \SO(n) \). The induced map \( \det^2 : G/H \to K \) is well-defined, bijective, and a homomorphism from \( G/H \to K \). Therefore it is an isomorphism from \( G/H \) to \( K \).

It is easily seen that \( (K, \cdot) \) is isomorphic to \( (\mathbb{Z}/2\mathbb{Z}, +) \) to construct an explicit isomorphic map, let \( \mathbb{Z}/2\mathbb{Z} = \{[0], [1]\} \) and define map \( \psi = \mathbb{Z}/2\mathbb{Z} \to K = \{\pm 1\} \) via \( \psi([j]) = (-1)^j \) for \( j = 0, 1 \). This is obviously well-defined bijection since \( \psi([0]) = 1, \psi([1]) = -1 \); it is also a homomorphism because

\[
\psi([0] + [0]) = \psi([0]) = 1 = 1 \cdot 1 = \psi([0]) \cdot \psi([0])
\]

\[
\psi([0] + [1]) = \psi([1]) = -1 = -1 \cdot 1 = \psi([1]) \cdot \psi([0])
\]

\[
\psi([1] + [1]) = \psi([0]) = 1 = -1 \cdot (-1) = \psi([1]) \cdot \psi([1])
\]

Therefore \( \psi \) is an isomorphism and \( (\mathbb{Z}/2\mathbb{Z}, +) \cong (K, \cdot) \).

4. \( O(n) \) is a semi direct product if we can find a subgroup \( M \) such \( M \cap \SO(n) = \{\Id\} \), \( M \cdot \SO(n) = \O(n) \). Obviously \( M \cong \O(n)/\SO(n) = \mathbb{Z}/2\mathbb{Z} \) i.e. a subgroup of order 2 that is not contained in \( \SO(n) \) : but any matrix such as

\[
R = \begin{pmatrix}
-1 & 0 \\
0 & 1 \\
. & . \\
0 & 1
\end{pmatrix}
\]

(a reflection) will have \( R^2 = \Id \) and \( \det(R) = -1 \), so \( M = \langle R \rangle \) has \( M \cap \SO(n) = \{\Id\} \). We have already noted that \( \SO(n) \cdot M = M \cdot \SO(n) = \SO(n) \cup \langle R \rangle \cdot \SO(n) \) is all of \( \O(n) \). Therefore \( \O(n) \) is a semi direct product of the form \( \SO(n) \rtimes \mathbb{Z}/2\mathbb{Z} \).

Exercise 3:
Determine all the conjugacy classes in

1. \( G = D_5 \)
2. \( G = D_6 \).

Note: Similar results hold for any \( D_n \). The pattern of classes depends on whether \( n \) is even or odd and the case \( n = 2 \) is exceptional because \( D_2 \) is abelian.
Hints: As explained in the Notes, the subgroup $N = \langle \rho \rangle$ is normal in $D_n$ and there are just two coset $N$ and $N\sigma$. Try computing $C_\sigma$ for $g = \rho^k$ ($C_\sigma \subseteq N$) and $g = \rho^k\sigma$ ($C_\sigma \subseteq N\sigma$) separately. Use the multiplication laws worked in the Notes.

Solution:

1. $D_5 = \{\rho^i, \sigma^j : i \in \mathbb{Z}/5\mathbb{Z}, j \in \mathbb{Z}/2\mathbb{Z}\}$ with $\theta = 360/5 = 72^\circ$. The multiplication law is $(\rho^k\sigma^l) \cdot (\rho^r\sigma^s) = \rho^{k+(r-s)}\cdot \sigma^{l+s}$.

Case 1: $g = p'$. If $g = e$, $C_\sigma = \{e\}$. If $r \neq 0 \pmod{5}$ then for all $k \in \mathbb{Z}/5\mathbb{Z}$, $l \in \mathbb{Z}/2\mathbb{Z}$, we get $xgx^{-1} = \rho^k\sigma^l \cdot \rho^r \cdot (\rho^k\sigma^l)^{-1} = [\rho^{k+(r-s)}] \cdot \sigma^l \cdot \rho^{-k} = \rho^{k+(r-s)}\cdot \sigma^{l+s}$. For instance if $r \equiv 0 \pmod{5}$ the elements of $N$ fall into 2-points conjugacy classes $C_{p'} = \{p'\} \cup \{p^{-r}\} \quad 1 \leq r \leq 2$. If $C_p = \{p\} \cup \{p^{-1}\}$ and $C_{p^2} = \{p^2\} \cup \{p^{-2}\} = \{p^2\} \cup \{p^3\}$ in $N = \{e, \rho, \rho^2, \rho^3, \rho^4\}$. When $r = 0$, we get trivial class $C_e = \{e\}$.

Case 2: $g = \rho\sigma$. Now $xgx^{-1} = \rho^k\sigma^l \cdot \rho\sigma \cdot \rho^k\sigma^l = \rho^{k+(r-s)}\cdot \sigma^{l+s} = \rho^{k+(r-s)}\cdot \sigma^l \cdot \rho^{-k} = \rho^{k+(r-s)}\cdot \sigma^l \cdot \rho^{-k}$. Hence $x \rightarrow \sigma^x \rightarrow \sigma^x \cdot \sigma\sigma^{-1}$ is an automorphism so $\sigma\rho\sigma^{-1} = (\sigma\rho\sigma^{-1})^{-k} = \rho^k \cdot \sigma = \rho^{k+(-1)^r} \cdot \sigma$ and in this case $C_{\rho,\sigma} = \{\rho^{2k+(-1)^r} \cdot \sigma : k \in \mathbb{Z}, l \in \mathbb{Z}\}$. For instance if $r = 0$, we have $g = \rho^{0}\sigma = \sigma$ and its conjugacy class consists of the elements $\rho^{2k}\sigma, k \in \mathbb{Z}$. These fill the entire coset $N\sigma$, so there are no other classes with representative $\rho^{2k}\sigma$.

$C_{\sigma} = \{\sigma, \rho^{2}\sigma, \rho^{4}\sigma, \rho^{6}\sigma = \rho\sigma, \rho^{8}\sigma = \rho^{3}\sigma\}$

with $\rho^{10}\sigma = \sigma\sigma = \sigma$.

$\{\sigma, \rho\sigma, \rho^{2}\sigma, \rho^{3}\sigma, \rho^{4}\sigma\} = (all \ of \ the \ coset \ N\sigma)$

The classes in $D_5$ have sizes $1, 2, 2 \ (in \ N)$ and $5 \ (all \ of \ N\sigma)$.

2. Again we consider 2 cases.

Case 1: $g = p' \in N$. If $r \equiv 0 \pmod{6}$, $g = e$ and $C_e = \{e\}$ (1-point class. If $g = p' \in N$ with $r \neq 0 \pmod{6}$, we again have $C_{p'} = \{p^{(-1)^r} : l \in \mathbb{Z}\} = \{p', p^{-r}\}$. Now, because 6 is even, it is possible to have $p' = p^{-r}$, resulting in another 1-point class. Indee if $r = 3$, $\rho^r = \rho^3 = \rho^{-3}$ has $C_\sigma = \{\rho^3\}$ and $g = \rho^3$ is in $Z(D_6)$, as is $e$. If $r = 1, 2$ the class $C_{p'}$ consists of 2 distinct points $\{\rho, \rho^{-1}\} = C_\rho$, $\{p^2, p^{-2}\} = C_{p^2}$. This accounts for all classes contained in $N$.

Case 2: $g = \rho\sigma \in N\sigma$. Same calculation yields

$C_{\rho,\sigma} = \{\rho^{2k+(-1)^r} \cdot \sigma : k \in \mathbb{Z}, l \in \mathbb{Z}\}$

but now we get 2 distinct conjugacy classes in $N\sigma$.

$C_{\sigma} = \{\sigma, \rho^{2}\sigma, \rho^{4}\sigma\}$

with $\rho^6\sigma = \sigma$

$C_{\rho,\sigma} = \{\rho\sigma, \rho^3\sigma, \rho^5\sigma\}$

with $\rho^7\sigma = \rho\sigma$.

The classes have size $1, 2, 2 \ (in \ N)$ and $3, 3 \ (in \ N\sigma)$. 

5
Exercise 4:
In \( G = D_n \), the geometric meaning of the rotation \( \rho^j_\theta \) and the reflection \( \sigma \) are clear. What are the geometric descriptions of the following group elements? (Assume \( n \leq 3 \).)

1. \( \rho_\theta \sigma \);
2. \( \rho^k_\theta \sigma \), when \( k \neq 0 \pmod n \)?
3. \( \rho^j_\theta \sigma \rho^{-j}_\theta \) when \( j \neq 0 \pmod n \)?

Hint: Every element \( \rho^j_\theta \sigma \in D_n \) in which the reflection \( \sigma \) appears is again a reflection \( r_\phi \) across a line \( l_\phi \) through the origin that makes the angle \( \phi \) with the \( +x \)-axis. Every point on this line of reflection symmetry remains fixed under \( r_\phi \); if you find the line with this property, you have determined \( r_\phi = \rho^j_\theta \sigma \).

Solution:
Geometric description (recall relations \( \sigma^2 = e, \rho \sigma^n = e, \sigma \rho \sigma^{-1} = \sigma \rho_\theta \sigma = \rho_{-\theta} = \rho^{-n-1}_\theta \) in \( D_n \)).

1. \( \rho_\theta \sigma \) acts on a base. This is a reflection across the line \( l_\phi \) making some angle \( \phi \) with the \( x \)-axis. This line will be left fixed by \( \rho_\theta \sigma \) and the reflection \( r_\phi \) across \( l_\phi \) the line. It is easy to see that the angle \( \phi \) must be \( \phi = \theta/2 \); The unit vectors go to the right place when reflected across this line and since we are dealing with linear operators on \( \mathbb{R}^2 \) we see that \( \rho_\theta \sigma = r_{\theta/2} \) = (reflection across the line \( l_{\theta/2} \) making angle \( \theta/2 \) with \( x \)-axis.)

Notice that the rotation \( \rho_\theta \) cyclically permutes the vertices of the \( n \)-gon; the reflection \( \sigma \) reflects across the \( x \)-axis, a line from origin through a vertex; the reflection \( r_{\theta/2} = \rho_\theta \sigma \) reflects across a line \( l_{\theta/2} \) from the origin to the midpoint of an edge of the \( n \)-gon.

2. \( \rho^k_\theta \sigma \) = reflection across a line, \( l_\phi \) making angle \( \phi \) with \( x \)-axis. We claim

- \( k = 1, \phi = \theta/2, \rho_\theta \sigma = \) reflection across line from center \( 0 \) to midpoint of first face;
- \( k = 2, \phi = \theta, \rho_\theta \sigma = \) reflection across line from center \( 0 \) to first vertex;
- \( k = 1, \phi = -3/2\theta, \rho^3_\theta \sigma = \) reflection across line from center \( 0 \) to midpoint of 2nd face;
- ... in the \( n \)-gon. To verifies this note how a line \( l_\phi \) gets mapped under successive operations:

\[
\begin{align*}
  l_\phi \xrightarrow{a} l_{-\theta} \xrightarrow{\rho_\theta} l_{-\phi + \theta} \xrightarrow{\rho_\theta} l_{-\phi + k\theta}
\end{align*}
\]

For the line to remain fixed we need \( l_\phi = l_{-\phi + k\theta} \) or \( 2\phi = k\theta, \phi = k\theta/2 \). We seem to have a paradox on our hands: the \( n \)-gon has \( n \) faces, \( n + 1 \) vertices; aren’t there \( 2n + 1 \) lines of reflection symmetry? But for \( 0 \leq j < n \), we get only \( n \) reflections \( \rho^j_\theta \sigma \). Solution: when \( n \) is even the faces come in pairs with same line through midpoints; for \( n \) odd each vertex lies opposite a face. In either case, there are only \( n \) lines of reflection symmetry for the \( n \)-gon.
3. Evaluate $\rho_j^j \sigma \rho^{-j}_0 = \rho_j \sigma \rho^{-j}_0$ by rewriting as $\rho_0^k \sigma$ as in 2. To do this remember $(\sigma = \sigma^{-1})$. So

$$\rho_j \sigma \rho^{-j}_0 = \rho_j (\sigma \rho_0^j) \cdot \sigma$$

Then there is a subgroup $H$ of $G$ that is normal in $G$. Hence

$$\rho_j \sigma \rho_0^j \sigma = \rho_j \sigma \rho_0^j \sigma$$

This, by 2, is reflection across line $l_\phi$ making angle $\phi = 2j\theta$ with x-axis. Geometrically, that is the line from center to the $j^{th}$ vertex.

This $D_n$ includes (in addition to reflection $\sigma$ across x-axis) all reflection

(a) line from origin to any vertex of $n$-gon ($\phi$ a multiple of $\theta$).

(b) line from origin to midpoint of any face ($\phi$ a $1/2$ integer multiple of $\theta$).

(some of these reflections may coincide, as we noted above.)

Exercise 5:

Prove that the exceptional dihedral group $D_2$ is isomorphic to the abelian group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution:

Analysis of $D_2 = \langle \rho_0, \sigma \rangle$ with $\rho_0 = 180^\circ$ rotation, $\sigma = $ reflection across x-axis. Here

$$\sigma \rho_0 \sigma = \rho_0$$

so $\sigma \rho_0 = \sigma \rho_0$, which means the generators commute when $n = 2$. This makes $D_2$ abelian, $|D_2| = 4$. There is two normal subgroups $A = \langle \rho_0 \rangle$, $B = \langle \sigma \rangle$, each order 2, with $A \cap B = \{e\}$ and $AB = D_2$. That implies $D_2$ is the direct product $D_2 \cong A \times B = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Every element in $D_2$ (except $e$) is of order 2. Multiplication table : $D_2 = \{e, \rho_0, \sigma, e\}$ with $c = \rho_0 \sigma = \sigma \rho_0 = $ reflection across the line through origin making angle $90^\circ$ with x-axis; i.e. the element of $D_2$ are $e, \sigma = $reflection across x-axis, $\sigma' = $reflection across y-axis, $\rho_0 = 180^\circ$ rotation $= \sigma \sigma'$? Note that $D_2$ is not isomorphic $\mathbb{Z}/4\mathbb{Z}$ because no $a \in D_2$ has $o(a) = 4$. Exercise 6:

Try to determine all groups with $|G| = 8$, up to isomorphism.

Note: This is a hard problem, but it is instructive even if you are only partially successful. You might organize your work into cases according the highest order $o(a)$ of any element in $G$, e.g. Case 1= (there is a a such that $o(a) = 8$); Case 2= (there is a a such that $o(a) = 4$ but no element has order 8); Case 3= (all elements $a \neq e$ have order equal to 2).

Solution: Case 1: there is a such that $o(a) = 8$. Then $G = \langle a \rangle = \langle \mathbb{Z}/8\mathbb{Z}, + \rangle$.

Case 2: there is a such that $o(a) = 4$, but no element of order 8.

Then there is cyclic subgroup $H$ with $H = \langle a \rangle = \mathbb{Z}/4\mathbb{Z}$. Note that $|G/H| = |G|/|H| = 2$, which by an easier exercise implies that $H$ is normal in $G$. Now take any $b \in G \setminus H$. The quotient map $\pi : G \to G/H \cong \mathbb{Z}/2\mathbb{Z}$ is a homomorphism and $\bar{b} = \pi(b) \neq \bar{c} = \pi(e)$. ($\bar{e} = $ the unit in $G/H$) since $b \notin H$. But $(b\bar{c})^2 = \bar{c}$ and $(b\bar{c})^2 = \pi(b) \cdot \pi(b) = \pi(b^2)$, hence we have $b^2 \in \ker(\pi) = H$. The possibilities are $b^2 = e, b^2 = a, b^2 = a^2, b^2 = a^3$. Since $H = \{e, a, a^2, a^3\}$. We analyze these cases as follows:

Case 2A : $b^2 = e$. Then $B = \langle b \rangle = \{e, b\}$ is a subgroup and $B \cap H = \{e\}, BH = G$
(because $|BH| = |B| \cdot |H|/|B \cap H| = 4 \cdot 2 = 8$), so at the very least $G$ is a semi direct product $G = H \times B \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in case 2A.

Case 2A.1: $b$ commute with $a$. Then $G$ is abelian and we have a direct product $G \simeq H \times B \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Case 2A.2: $b$ does not commute with $a$ (the generator of $H$). Look at the action of $B$ on $H$ by automorphism $\phi_0: h \mapsto bhb^{-1}$. Thus is nontrivial if $b$ does not commute with $a$. Since $H \simeq \mathbb{Z}/4\mathbb{Z}$, the automorphism $\phi_b \neq \text{id}$ in $\text{Aut}(\mathbb{Z}/4\mathbb{Z})$ has the form $\phi_b: [l] \mapsto [k][l]$ for some $1 \leq k \leq 3$ such that $[k] \in U_4$ i.e. $\gcd(k, 4) = 1$. The only possibilities are $\phi_b = \phi_{[1]} = \text{Id}$ (which has been excluded as case 2A.1) and $\phi_b = \phi_{[3]}$. Since $[3] = -[1]$ in $\mathbb{Z}/4\mathbb{Z}$, $\phi_{[3]}[l] = -[l]$, $\forall l \in \mathbb{Z}/4\mathbb{Z}$, and $\phi_b$ is the inversion $\phi_b: g \mapsto g^{-1}$ in $H$. Since $(\phi_b)^2 = \text{id}_H$, the map $\Phi: B \rightarrow \text{Aut}(H)$ such that $\phi_b = \text{(inversion)}$ really is a homomorphism and we get a nontrivial action of $B \simeq \mathbb{Z}/2\mathbb{Z}$ on $H \simeq \mathbb{Z}/4\mathbb{Z}$. Hence, we get a non commutative semi direct product $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ whose group law can be written explicitly in term of $\phi: \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/4\mathbb{Z})$: Every $g \in G = HB$ can be written uniquely as $g = h_1h_2$ and the multiplication laws becomes

$$(h_1, b_1) \cdot (h_2, b_2) = h_1(h_1h_2b_1^{-1})b_1b_2 = [h_1\phi_{b_1}(h_2)] \cdot [b_1b_2]$$

where $\phi_{b_1}(h_2)$ if $b_1 = e$ and $\phi_{b_1}(h_2) = h_2^{-1}$ if $b_1 = b$ in $B = < b > \simeq \mathbb{Z}/2\mathbb{Z}$. You might recognize this group as $D_4$; if you identify $\rho_0 = a$, $\sigma = b$ ($\theta = 2\pi/4$ radians), you will see that $G$ and $D_4$ have exactly the same multiplication law.

Case 2B: $b^2 = a$ (If $b^2 = a^3 = a^{-1}$. The discussion is the same since $a$ and $a^3$ both generate $H = \mathbb{Z}/4\mathbb{Z}$). Distinct $G = H \cup bH$ (disjoint cosets) since $|G/H| = 2$. But $H = \{ e, a, a^2, a^3 \}$ and $bH = \{ b, ba, ba^2, ba^3 \}$. Then we get distinct elements $\{ e, b, b^2 = a, b^3 = ba, b^4 = b^2a = a^2, b^5 = ba^2, b^6 = a^3, b^7 = ba^3 \}$ and $b^8 = a^4 = e$. This would imply $o(b) = 8$, which impossible. Thus case cannot occur!

Case 2C: $b^2 = a^2$. Then the elements $\{ e, b, b^2 = a^2, b^3 = ba^2 \}$ are distinct and $b^4 = (a^2)^2 = e$ so $|B| = 4 = o(b)$ and $B \simeq \mathbb{Z}/4\mathbb{Z}$ with $H \cap B = \{ e, a^2 \} \simeq \mathbb{Z}/2\mathbb{Z}$. Although $b$ has order 4. There might exist $b' \in bH$ such that $o(b') = 2$. If so we would have $B' = < b' >$ a subgroup of order 2 such that $B' \cap H = \{ e \}$ and $B'H = G$. Then $G$ is a semi direct product $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ and we are block in Case 2A. If such $b'$ does not exist we have a new group for our list. We determine whether $b'$ exists by examining consequences of the relations $a^4 = b^4 = e$ and $a^2 = b^2$; note that $b'$ must be one of the elements in the coset $bH = \{ b, ba, ba^2, ba^3 \}$ in order to have $B' \cap H = \{ e \}$. We get 2 sub cases according to whether $b'$ commutes with $b$.

Case 2C.1: $b'$ commutes with $b$. Take $b' = ab$. Then $(ab)^2 = abab = a^2b^2 = a^4 = e$ as required.

Case 2C.2: $ab \neq ba$. Then $ab$ belongs to the coset $bH$ because $H \leq G$ implies $abH = aHb = Hb = bH$, so $ab$ must be equal to one of the elements in $bH = \{ b, ba, ba^2, ba^3 \}$. We can quickly eliminate $ab = b$ (implies $a = e$ a contradiction); $ab = ba$ (that is Case 2C.1), $ab = ba^2$ (implies $ab = b^3 \Leftarrow a = b^2 = a^2 \Leftarrow a = e$ a contradiction) Thus only remaining possibility is $ab = ba^3$. Then $ab = ba^{-1}$ and $aba = b$; similarly $bab^2 = a$ (because $aba = b \Leftarrow abab^{-1} = e \Leftarrow bab^{-1} = a^{-1} \Leftarrow a^3 \Leftarrow bab^3 = a^5 \Leftarrow bab^2 = ab^2 \Leftarrow bab = a$). Now we get $(ab)^2 = abab = b^2 \neq e$; $(ba)^2 = babab = a^2 \neq e$; $(ba^2)^2 = ba^2ba^2 = ba(ab)a = baba = b^2 \neq e$; $(ba^3)^2 = ba^3ba^3 = b^3babab^2 = b^3b^2 = b^6 = b^2 \neq e$.

Thus, no $b' \in bH$ can have order 2, and in this case we get a new non-commutative
Note : we can’t have $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ with $\mathbb{Z}/2\mathbb{Z} \leq G$ either. The group of automorphism of $(\mathbb{Z}/2\mathbb{Z}, +)$ is trivial, hence the only possible action of $\mathbb{Z}/4\mathbb{Z}$ by automorphism on $\mathbb{Z}/2\mathbb{Z}$ is trivial, so we only get the direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ already listed.

It is commonly described as the set of symbols $\{\pm 1, \pm i, \pm j, \pm k\}$ which are multiplied by the following rules (note that the group operations do not commute):

1. $\pm 1$ have the usual behavior: they commute with everybody,
   
   $1 \cdot x = x, (-1)(\pm x) = \mp x, \forall x; (-1)^2 = 1, 1^2 = 1$

2. usual rules of signs hold $(+x)(-y) = (-x)(+y) = -(xy)$ and $(-x)(-y) = xy$.

3. $i^2 = j^2 = k^2 = -1$ (so $i, j, k$ each behave like $\sqrt{-1}$ in $\mathbb{C}$)

4. $ij = k$, $jk = i$, $ki = j$ (note the cyclic order in this rule.)

5. $ij = -ji$, $ik = -ki$, $jk = -kj$ (anti-commutation relations for $i, j, k$)

If you take $a = i$, then $H = \langle a \rangle = \{1, i, -1, -i\} \simeq \mathbb{Z}/4\mathbb{Z}$; and if you take $b = j$ you get $B = \langle b \rangle = \{1, j, -1, -j\}$ with $H \cap B = \{\pm 1\}$. It is easily verified that $HB = G$; in fact $bH = \{j, ji, ji^2, ji^3\} = \{j, -k, -j, k\}$ picks up $\pm k$. Clearly $ab \neq ba$ and $a^2 = b^2(= -1)$ as required to put us into Case 2C.2.

One case remains; it is fairly easy.

Case 3 : $o(a) = 2$, $\forall a \neq e$ : First of all $G$ is commutative: if $x, y \in G$ then $e = (xy)^2 = x(x^{-1}yx) = e(yx) = (yx)^2 = y(xy)$ so $x \in H_3$. Pick $a \neq e$; $H_1 = \langle a \rangle$ is order 2. Pick $b \notin H_1$; then $H_2 = \langle b \rangle$ has order 2 and $H_1 \cap H_2 = \{e\}$ such that $H_1H_2 = H$ has $|H| = 4$ and $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Finally pick $c \notin H$. Then $c^2 = e$ so $H_3 = \langle c \rangle$ has $H_3 \cap H = \{e\}$, $H_3H = G$ and $G \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in this case.

To summarize. If $|G| = 8$, $G$ is isomorphic to one of the following groups

1. $\mathbb{Z}/8\mathbb{Z}$;

2. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

3. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;

4. The group of quaternion units (Case 2C.2) $\{\pm 1, \pm i, \pm j, \pm k\}$;

5. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with the nontrivial element $b \in \mathbb{Z}/2\mathbb{Z}$ acting on $\mathbb{Z}/4\mathbb{Z}$ by the automorphism $\phi_b(a^k) = a^{-k}$ (i.e. in additive notation, $\phi_b([k]) = -[k], k = 0, 1, 2, 3.$) (This is isomorphic to the dihedral group $D_4$.)

I leave it to you to explain why items 1., 2., 3. cannot be isomorphic.