Determine all finite subgroups of $C^*$, the group of non-zero complex numbers under multiplication

Grader’s Notes:

- MPC means you must “must prove cyclic”, in any group every element $g$, $g$ generates a cyclic sub-group; in fact in $C^*$ there is a sub-group $S^1 = \{ z \in C : |z| = 1 \}$, which is not generated by a root of unity but for which every $z \in S^1$ is a root of unity. $S^1$ however, is infinite, not finite, we can write $z = e^{i\theta}$ and for each $\theta \in [0,2\pi)$ there is exactly one $z = e^{i\theta}$ and there are infinitely many choices for $\theta \in [0, 2\pi)$.
- Related to the above remark about $S^1$; it is necessary that $|z| = 1$ for all $z \in G$ if $G$ is finite, but it is not sufficient.
- Also related to the MPC remark, it’s not enough to just show that every element of $G$ is a root of unity for some $n$, you should show that the elements of $G$ are all $n$-th roots of unity for some particular $n$ (which will be $n = |G|$), it’s possible to do this by appealing to the fundamental theorem of algebra or directly. If you appeal to the fundamental theorem of algebra, there is a necessary combinatorial argument require to show that $G$ is in fact the group of all $|G|$-th roots of unity.

Example Solution:

Suppose $G \subseteq C^*$ with $|G|$ finite. By corollary 4 of Lagrange’s Theorem (p 143) you know that for all $z \in G$, $z^{|G|} = 1$, since 1 is identity in $C^*$. By the fundamental theorem of algebra, $z^{|G|} = 1$ has $|G|$ solutions in $C^*$, since $G$ has $|G|$ elements, and each element of $|G|$ is a $|G|$-th root of unity, of which there are $|G|$ it follows that $G = \{ z \in C^* : z$ is a $|G|$-th root of unity $\}$.

If you would like to show this without appealing directly to the fundamental theorem of algebra, you can. (But it’s a bit involved) An $n$-th root of unity has the form $e^{ik\pi/n}$ where, without loss of generality, $k = 1, \ldots, 2n - 1$. Furthermore, without loss of generality you can choose $n, k$ to be relatively prime. Since $G$ is finite you can choose $z \in G$ such that $z = e^{ik\pi/n}$ where $n$ is greatest amongst all such $z \in G$, since $\langle z \rangle \leq G$ and $k, n$ are relatively prime, you find that $z_1 = z^{n-k+1} = e^{im\pi/n} \in G$. If $G \neq \{z\}$ then you can find $z' \in G$, $z' = e^{ik'\pi/n'}$ such that for all $m \in Z$, $z_0^{mn} \neq z', i.e. for all m \in Z e^{ik\pi/m} \neq e^{imk(n^m/n)}$, this means that $k, nn'$ are pairwise relatively prime, in particular that $z_0z' = e^{ik\pi/mn}$ has $k', mn$ relatively prime, but $mn > n$, contradicting the choice of $n$ to be the largest.

Suppose that $H$ and $K$ are subgroups of $G$ and there are elements $a$ and $b$ such that $aH \subseteq bK$ prove that $H \subseteq K$.

There are two solutions that were very common, the shorter is:

Example Solution:

Suppose that $aH \subseteq bK$, it follows that $H = a^{-1}H \subseteq a^{-1}bK$, note that $e \in H$, so $e \in a^{-1}bK$, since for any $e, d \in G$ either $cK \cap dK = \emptyset$ or $cK = dK$ and (note $K = eK$) $K \cap a^{-1}bK \neq \emptyset$ it follows that $K = a^{-1}bK \supseteq H$.

Here’s the other:

Example Solution:

Suppose that $aH \subseteq bK$, since $e \in H$ there is some $k \in K$ such that $a = ae = bk$ (else $aH \nsubseteq aK$). So $b^{-1}a = k$, so since $aH \subseteq bK$, $H = a^{-1}aH \subseteq a^{-1}bK = a^{-1}b(kK) = a^{-1}bb^{-1}aK = K$.
Grader’s Notes:

- Some students wanted to say that since \( \mathbb{Z}_3 \oplus \mathbb{Z}_3 \) and \( H \) have the same number of elements of each order, they are isomorphic, this is not true in general, though I haven’t been able to think of a counter-example for finite groups, this is certainly not true for infinite groups; \( \mathbb{Z} \) and \( \mathbb{Q} \) have countably many elements of infinite order and only 2 elements of finite order, but are non-isomorphic. There should be an example for finite groups, in a counter-example for finite groups, at least one group must be non-Abelian.

Example Solution:

The first step of showing \( H \) is a group is to show that \( H \) is closed under the operation:

\[
H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : a, b \in \mathbb{Z} \right\}
\]

Show that \( H \) is an Abelian group of order 9. Is \( H \) isomorphic to \( \mathbb{Z}_9 \) or to \( \mathbb{Z}_3 \oplus \mathbb{Z}_3 \)?

\[
H \to \mathbb{Z}_3 \oplus \mathbb{Z}_3
\]

\[\begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} (1 \cdot 1 + a_1 \cdot 0 + b_1 \cdot 0) & (1 \cdot a_2 + a_1 \cdot 1 + b_1 \cdot 0) & (1 \cdot b_2 + a_1 \cdot 0 + b_1 \cdot 1) \\ (0 \cdot 0 + 1 \cdot 0 + 0 \cdot 0) & (0 \cdot a_2 + 1 \cdot 1 + 0 \cdot 0) & (0 \cdot b_2 + 1 \cdot 0 + 0 \cdot 1) \\ (0 \cdot 0 + 0 \cdot 0 + 1 \cdot 0) & (0 \cdot a_2 + 0 \cdot 1 + 1 \cdot 0) & (0 \cdot b_2 + 0 \cdot 0 + 1 \cdot 1) \end{bmatrix}
\]

\[\begin{bmatrix} 1 & a_1 + a_2 & b_1 + b_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & b_1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}
\]

It may already be obvious to you that \( H \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \). Now while we could verify that this is a group by computational finding inverses and checking associativity, I refer to a past solution where I point out that if you construct a bijective map \( \phi : G_1G_2 \) where \( \phi(ab) = \phi(a)\phi(b) \) and \( G_2 \) is a group, then \( G_1 \) is a group. So we construct \( \phi : H \to \mathbb{Z}_3 \oplus \mathbb{Z}_3 \) by:

\[
\phi \left( \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \right) = (a, b)
\]

We check that \( \phi \) respects the operation:

\[
\phi \left( \begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix} \right) = \phi \left( \begin{bmatrix} 1 & a_1 + a_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} b_1 + b_2 \\ 0 \end{bmatrix} \right) = \phi \left( \begin{bmatrix} a_1 + a_2, b_1 + b_2 \\ 0, 0 \end{bmatrix} \right) = (a_1 + a_2, b_1 + b_2) = (a_1, b_1) + (a_2, b_2)
\]

\[
\phi \left( \begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b_1 \\ 0 & 1 \end{bmatrix} \right) + \phi \left( \begin{bmatrix} 1 & a_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b_2 \\ 0 & 1 \end{bmatrix} \right) = \phi \left( \begin{bmatrix} a_1 \\ 0 \\ 0 \end{bmatrix} \right) + \phi \left( \begin{bmatrix} a_2 \\ 0 \\ 0 \end{bmatrix} \right) = (a_1, b_1) + (a_2, b_2)
\]
\( \phi \) is bijective because \( \phi \) has an inverse:
\[
\phi^{-1}(a, b) = \begin{bmatrix}
1 & a & b \\
0 & 1 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}
\]

So \( \phi \) is an isomorphism.

\( H \) is not isomorphic to \( \mathbb{Z}_9 \) because every element of \( H \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \) has order 1 or 3 while \( \mathbb{Z}_9 \) has an element of order 9.

An alternate proof that \( H \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \) could be given by showing the groups:
\[
H_1 = \left\{ \begin{bmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : a \in \mathbb{Z}_3 \right\} \quad H_2 = \left\{ \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : b \in \mathbb{Z}_3 \right\}
\]
are sub-groups of \( H \), and \( H_1 \cap H_2 \) is the trivial subgroup of \( H \), then showing that \( H_1 \times H_2 = H \), so \( H \cong H_1 \oplus H_2 \) and showing that \( H_1, H_2 \cong \mathbb{Z}_3 \); though to be very careful, one also needs to show that if \( G_1 \cong G_1' \) and \( G_2 \cong G_2' \) then \( G_1 \oplus G_2 \cong G_1' \oplus G_2' \). \( \square \)