Homework 7 Solution
Chapter 7 - Cosets and Lagrange’s theorem.
due: Oct. 31.

1. Find all left cosets of $K$ in $G$.

(a) $G = \mathbb{Z}$, $K = \langle 4 \rangle$.

\[ K = \{ 4m \mid m \in \mathbb{Z} \}, \quad 1 + K = \{ 4m + 1 \mid m \in \mathbb{Z} \}, \]
\[ 2 + K = \{ 4m + 2 \mid m \in \mathbb{Z} \}, \quad 3 + K = \{ 4m + 3 \mid m \in \mathbb{Z} \}. \]

(b) $G = U(9)$, $K = \langle 8 \rangle$.

In this case, $|U(9)| = 6$ and $|K| = |8| = 2$. So there are $6/2 = 3$ distinct cosets.

\[ K = \{ 1, 8 \}, \quad 2K = \{ 2 \cdot 1, 2 \cdot 8 \} = \{ 2, 7 \}, \quad 4K = \{ 4 \cdot 1, 4 \cdot 8 \} = \{ 4, 5 \}. \]

(c) $G = D_4$, $K = \langle H \rangle$.

Note that there are $|D_4|/|K| = 8/2 = 4$ distinct cosets.

\[ K = \{ R_0, H \}, \quad R_{90}K = \{ R_{90}R_0, R_{90}H \} = \{ R_{90}, D' \}, \]
\[ R_{180}K = \{ R_{180}R_0, R_{180}H \} = \{ R_{180}, V \}, \quad R_{270}K = \{ R_{270}R_0, R_{270}H \} = \{ R_{270}, D \}. \]

(d) $G = A_4$, $K = \{ e, (12)(34), (13)(24), (14)(23) \}$.

The order of $A_4$ is 12 and $|K| = 4$. So there are 3 distinct cosets.

\[ K, \quad (123)K = \{ (123)e, (123)(12)(34), (123)(13)(24), (123)(14)(23) \} = \{ (123), (134), (243), (142) \}, \]
\[ (132)K = \{ (132)e, (132)(12)(34), (132)(13)(24), (132)(14)(23) \} = \{ (132), (234), (124), (143) \}. \]

2. Let $G = GL(2, \mathbb{R})$ and $H = SL(2, \mathbb{R})$. For $A \in GL(2, \mathbb{R})$, show that

\[ AH = \{ B \in GL(2, \mathbb{R}) \mid \det B = \det A \}. \]

Let $X = \{ B \in GL(2, \mathbb{R}) \mid \det B = \det A \}$. If $B \in AH$, then there exists $C \in H$ such that $B = AC$. Then $\det B = \det(AC) = (\det A)(\det C) = \det A$ because $C \in H = SL(2, \mathbb{R})$. So $B \in X$ and $AH \subset X$.

Conversely, if $B \in X$, then $\det(A^{-1}B) = \det(A^{-1}) \det B = (\det A)^{-1} \det B = (\det A)^{-1}(\det A) = 1$ and $A^{-1}B \in H$. Therefore $B = AA^{-1}B \in AH$ and $X \subset AH$. Thus $X = AH$. 

3. Let \( H \) be a subgroup of \( G \) and \( a, b \in G \).

(a) Show that \( aH = Ha \) if and only if \( H = aHa^{-1} \).

Sol 1. Suppose that \( aH = Ha \). Then for any \( h \in H \), \( ha \in Ha = aH \). So there is \( h' \in H \) such that \( ha = ah' \). So \( h = ah'a^{-1} \in aHa^{-1} \). Therefore \( H \subset aHa^{-1} \). Also for every \( aha^{-1} \in aHa^{-1} \), \( ah \in aH = Ha \), so there is \( h'' \in H \) such that \( ah = h''a \). Then \( aha^{-1} = h''a^{-1} = h'' \in H \). So \( aHa^{-1} \subset H \). Therefore we can conclude that \( aHa^{-1} = H \).

Conversely, assume that \( H = aHa^{-1} \). Then for every \( ah \in aH \), \( aha^{-1} \in aHa^{-1} = H \), so there is \( h' \in H \) such that \( aha^{-1} = h' \). Then \( ah = aha^{-1}a = h'a \in Ha \). Therefore \( aH \subset Ha \). For any \( ha \in Ha \), \( h \in H = aHa^{-1} \), so there is \( h'' \in H \) such that \( h = ah''a^{-1} \). Now we have \( ha = ah''a^{-1}a = ah'' \in aH \). So \( Ha \subset aH \). Therefore \( aH = Ha \).

Sol 2. This is a more concise solution. (But you have to convince yourself on each step! This solution is very illusive because each equality is not that of elements, but that of sets.)

If \( aH = Ha \), then \( H = Haa^{-1} = aHa^{-1} \). Conversely, if \( H = aHa^{-1} \), then \( aH = aHa^{-1}a = Ha \).

(b) Show that \( aH = bH \) if and only if \( Ha^{-1} = Hb^{-1} \).

Sol 1. Suppose that \( aH = bH \). Then \( a \in aH = bH \). So there is \( h \in H \) such that \( a = bh \). Then \( a^{-1} = (bh)^{-1} = h^{-1}b^{-1} \in Hb^{-1} \). This implies that \( Ha^{-1} = Hb^{-1} \).

Conversely, assume that \( H a^{-1} = H b^{-1} \). Then \( a^{-1} \in Ha^{-1} = H b^{-1} \). So there is \( k \in H \) such that \( a^{-1} = kb^{-1} \). Now \( a = (kb^{-1})^{-1} =bk^{-1} \in bH \). Therefore \( aH = bH \).

Sol 2. (Again, this solution is very dangerous if you don’t spend some time to understand the detail.)

If \( aH = bH \), then \( a \in aH = bH \), so \( a = bh \) for some \( h \in H \). Then \( Ha^{-1} = H(bh)^{-1} = Hh^{-1}b^{-1} = Hb^{-1} \).

If \( Ha^{-1} = Hb^{-1} \), then \( a^{-1} \in Ha^{-1} = Hb^{-1} \) and \( a^{-1} = hb^{-1} \) for some \( h \in H \).

\( a = (hb^{-1})^{-1} = bh^{-1} \in bH \). So \( aH = bH \).

4. Let \( G \) be a group such that \( |G| = p^n \) for some prime number \( p \) and a positive integer \( n \). Show that \( G \) has an element of order \( p \).

Take \( a \in G \) such that \( a \neq e \). By a corollary of Lagrange’s theorem, \( |a| \mid |G| = p^n \).

So \( |a| = p^k \) for some \( 1 \leq k \leq n \). Then \( |a^{p^{k-1}}| = p^k / p^{k-1} = p \). So \( a^{p^{k-1}} \) is what we want.

5. Let \( G \) be a group of order 245. Show that \( G \) has at most one subgroup of order 49.

Let \( H \) and \( K \) be two subgroups of order 49. Because \( H \cap K \leq H \), \( |H \cap K| \mid |H| = 49 \). So \( |H \cap K| = 1, 7, \) or \( 49 \). Then

\[
\frac{|HK|}{|H \cap K|} = \frac{|H||K|}{|H \cap K|} = \frac{49 \cdot 49}{|H \cap K|} = 7^4.
\]
6. Let $G$ be a group of order 35.

(a) Prove that $G$ must have an element of order 5.

If $G$ is cyclic and $G = \langle a \rangle$, then $|a^7| = 35/7 = 5$.

Now suppose that $G$ is not cyclic, then every element has the order 1, 5, or 7. Also the only one element of order 1 is $e$. For two nonidentity elements $a,b \in G$ of order 7, $\langle a \rangle \cap \langle b \rangle \leq \langle a \rangle$ so $|\langle a \rangle \cap \langle b \rangle|/|\langle a \rangle| = 7$. Therefore if $\langle a \rangle \neq \langle b \rangle$, $|\langle a \rangle \cap \langle b \rangle| = 1$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$. Furthermore, in $\langle a \rangle$, except $e$, all other elements have order 7 so there are 6 elements of order 7 in $\langle a \rangle$. In summary, the number of order 7 elements in $G$ is $6k$ for some $k \in \mathbb{N}$. Now $|G - \{e\}| = 34$ is not the multiple of 6. Therefore there must be an element of order 5.

(b) Show that $G$ has an element of order 7.

If $G$ is cyclic and $G = \langle a \rangle$, then $|a^5| = 35/5 = 7$.

If $G$ is not cyclic, then by the same argument in the previous problem, we can see that the number of order 5 elements in $G$ is $4k$ for some $k \in \mathbb{N}$. But $|G - \{e\}| = 34$ is not a multiple of 4. Therefore there must be an element of order 7.

(c) Furthermore, assume that $G$ is Abelian. Show that $G$ is cyclic.

By (a) and (b), there are two element $a,b \in G$ such that $|a| = 5$, $|b| = 7$. We claim that $|ab| = 35$. Note that from $\langle a \rangle \cap \langle b \rangle \leq \langle a \rangle$, $|\langle a \rangle \cap \langle b \rangle|/|\langle a \rangle| = 5$. Similarly, we have $|(a) \cap (b)|/(|b|) = 7$. So $|(a) \cap (b)| = 1$ and $\langle a \rangle \cap \langle b \rangle = \{e\}$.

If $|ab| = n$, then $a^nb^n = (ab)^n = e$. So $a^{-n} = b^n \in \langle a \rangle \cap \langle b \rangle = \{e\}$. Thus $b^n = e$ and $7 = |b| | n$. And $a^n = (a^{-n})^{-1} = e^{-1} = e$, so $5 = |a| | n$. Therefore $n \geq \text{lcm}(7,5) = 35$. The maximum value of an order of $ab \in G$ is 35. So $|ab| = 35$ and $G = \langle ab \rangle$.

7. For the five platonic solids (tetrahedron, cube, octahedron, dodecahedron, icosahedron), compute the orders of their rotation groups.


Fix a vertex $v$. In every case, it is not difficult to check that every vertex can be moved to another vertex by several rotations. So for all of the five solids, there is only one orbit and the number of elements in the orbit is precisely the number of vertices. Therefore $|orb_{R_T}(v)| = 4$, $|orb_{R_C}(v)| = 8$, $|orb_{R_O}(v)| = 6$, $|orb_{R_D}(v)| = 20$, and $|orb_{R_I}(v)| = 12$. 

3
On the other hand, then the order of stablizer of \( v \) is precisely the number of faces adjacent to \( v \). So \( |\text{stab}_{R_T}(v)| = 3, |\text{stab}_{R_C}(v)| = 3, |\text{stab}_{R_O}(v)| = 4, |\text{stab}_{R_D}(v)| = 3, |\text{stab}_{R_I}(v)| = 5. \)

Therefore

\[
|R_T| = |\text{orb}_{R_T}(v)| \cdot |\text{stab}_{R_T}(v)| = 4 \cdot 3 = 12, \\
|R_C| = |\text{orb}_{R_C}(v)| \cdot |\text{stab}_{R_C}(v)| = 8 \cdot 3 = 24, \\
|R_O| = |\text{orb}_{R_O}(v)| \cdot |\text{stab}_{R_O}(v)| = 6 \cdot 4 = 24, \\
|R_D| = |\text{orb}_{R_D}(v)| \cdot |\text{stab}_{R_D}(v)| = 20 \cdot 3 = 60, \\
|R_I| = |\text{orb}_{R_I}(v)| \cdot |\text{stab}_{R_I}(v)| = 12 \cdot 5 = 60.
\]

Can you see an interesting pattern? Actually, the rotation group of a cube is isomorphic to that of an octahedron, and the rotation group of a dodecahedron is isomorphic to that of an icosahedron. Think about the reason.

8. By using Lagrange’s theorem and its corollaries, we can prove a lot of highly nontrivial facts on the structure of finite groups. Here is one example: Let \( H \) be a subgroup of order 60 in \( S_5 \). Note that \( |S_5| = 120 \). So there are only two left cosets of \( H \) in \( S_5 \), namely, \( H \) and \( \alpha H \) for some \( \alpha \notin H \).

(a) Show that all cycles of length 3 are in \( H \). (Hint: If a length 3 cycle \( \alpha \) is not in \( H \), then \( \alpha H \neq H \). \( \alpha^2 H \) must be one of \( H \) or \( \alpha H \).)

Let \( \alpha \) be a length 3 cycle. If \( \alpha \notin H \), then \( H \) and \( \alpha H \) are two distinct cosets and they are disjoint. Because \( |H| = 60 = |S_5|/2 \), there are only two distinct
cosets. Then \(\alpha^2 H\) is one of \(H\) and \(\alpha H\). If \(\alpha^2 H = H\), then \(\alpha^3 H = \alpha \alpha^2 H = \alpha H\). But \(\alpha^3 = e\) because it is a length 3 cycle, so \(\alpha^3 H = H\) and we have a contradiction. If \(\alpha^2 H = \alpha H\), then \(\alpha H = \alpha^{-1} \alpha^2 H = \alpha^{-1} \alpha H = H\). So we have another contradiction. So \(H\) must be equal to \(\alpha H\). In other words, \(\alpha \in H\).

(b) Show that all cycles of length 5 are in \(H\).

Now let \(\alpha\) be a length 5 cycle. If \(\alpha \not\in H\), then \(H\) and \(\alpha H\) are two distinct cosets. Then \(\alpha^2 H\) is one of \(H\) and \(\alpha H\). If \(\alpha^2 H = H\),

\[
\alpha H = \alpha^6 H = \alpha^2 \alpha^2 H = \alpha^2 \alpha^2 H = \alpha^2 H = H
\]

and we have a contradiction. If \(\alpha^2 H = \alpha H\), then \(\alpha H = \alpha^{-1} \alpha^2 H = \alpha^{-1} \alpha H = H\). So both cases are impossible and \(\alpha H = H\). This implies that \(\alpha \in H\).

(c) Count the numbers of length 3 cycles and length 5 cycles in \(S_5\).

To make a length 3 cycle, we need to choose 3 elements in \(\{1, 2, 3, 4, 5\}\). The number of such choices is \(5 \cdot 4 \cdot 3 = 60\). But there are some ambiguities, because three cycles \((abc), (bca), (cab)\) are same. Therefore the number of distinct length 3 cycles in \(S_5\) is \(60 / 3 = 20\).

Similarly, the number of ways to make a 5 cycle is \(5! / 5 = 24\). (We need to divide by 5 because the five cycles \((abcde), (bcdea), (cdeab), (deabc), (eabcd)\) are all same.

(d) By using Theorem 7.2 in the textbook, conclude that \(H = A_5\). (Hint: Note that length 3 cycles and length 5 cycles are all even permutations.)

Suppose that \(H\) is different from \(A_5\). Then \(H \cap A_5 \leq H\), so \(|H \cap A_5| \cdot |H| = 60\). But by (c), we already have \(20 + 24 = 44\) elements of \(H \cap A_5\). The only one divisor of 60 larger than 30 is 60. So \(|H \cap A_5| = 60\) and \(H = A_5\).

Therefore, there is only one subgroup \((A_5)\) of order 60 in \(S_5\).