Homework Assignment 6: Solutions

1. Let G be a group, and $M, N \trianglelefteq G$ normal subgroups such that $MN = G$.

   (a) Show $G/(M \cap N) \cong (G/M) \times (G/N)$

   Proof. We freely use the fact that for $g \in G$, $gM = M$ if and only if $g \in M$, and similarly for N, which follows from HW4#8(a).
   We build a homomorphism $\pi : G \to (G/M) \times (G/N)$ via the rule $\pi(g) = (gM, gN)$. This is clearly a homomorphism since:

   $$\pi(xy) = (xyM, xyN) = (xMyM, xNyN) = (xM, xN)(yM, yN) = \pi(x)\pi(y).$$

   We now observe that π is surjective. Fix (xM, yN) in the target. Since $MN = G$, there is $m \in M$ and $n \in N$ such that $x^{-1}y = mn$. Solving one gets $xm = yn^{-1}$, call this value g. Then:

   $$\pi(g) = (gM, gN) = (xmM, yn^{-1}N) = (xM, yN).$$

   Finally, notice that the kernel of π is the set of $g \in G$ such that $gM = M$ and $gN = N$. But this is precisely $M \cap N$. Therefore, the first isomorphism theorem gives the result. $\square$

   (b) Suppose further that $M \cap N = \{1\}$. Show that $G \cong M \times N$.

   Proof. We will find the following lemma useful.

   Lemma 1. *Suppose $H_1 \cong H_2$ and $K_1 \cong K_2$. Then $H_1 \times K_1 \cong H_2 \cong K_2$.*

   Proof. Let $\varphi : H_1 \to H_2$ and $\psi : K_1 \to K_2$ be isomorphisms. Then we build:

   $$\begin{aligned} \varphi \times \psi : H_1 \times K_1 &\longrightarrow H_2 \times K_2 \\ (h, k) &\mapsto (\varphi(h), \psi(k)). \end{aligned}$$

   It is easy to verify that $\varphi \times \psi$ is a homomorphism and that $(\varphi \times \psi)^{-1} = \varphi^{-1} \times \psi^{-1}$. $\square$

   Now to prove the result, we consider the diamond:

   $$\begin{tikzcd} & G = MN \arrow[dl, dash] \arrow[dr, dash] & \\ M \arrow[dr, dash] & & N \arrow[dl, dash] \\ & \{1\} = M \cap N & \end{tikzcd}$$

   By the second isomorphism theorem we have $G/M \cong N$ and $G/N \cong M$. Therefore, the result follows from the following chain of isomorphisms, where the first is part (a), and the second is the lemma.

   $$G \cong (G/M) \times (G/N) \cong N \times M.$$

   $\square$

2. Let G be a group and $Z(G)$ its center.

(a) Suppose $H \leq Z(G)$. Show that H is a normal subgroup of G. (In particular, $Z(G)$ is normal).

Proof. Fix $z \in H$ and $g \in G$. It suffices to show $gzg^{-1} \in H$. But since $z \in Z(G)$ we have $gzg^{-1} = gg^{-1}z = z \in H$, so we are done. □

(b) Show that if $G/Z(G)$ is cyclic, then G is abelian.

Proof. If $G/Z(G)$ is cyclic then we can fix a generator: $G/Z(G) = \langle xZ(G)\rangle$. Then the cosets $x^iZ(G)$ for $i \in \mathbb{Z}$ form a partition of G. In particular, fix $a, b \in G$. Then $a = x^iz$ and $b = x^jw$ for $z, w \in Z(G)$. Therefore we can leverage that we can freely commute with z and w, and x^i and x^j commute with eachother to conclude that

$$ab = x^izy^jw = zx^ix^jw = zx^jx^iw = x^jzwx^i = x^jwzx^i = x^jwx^iz = ba.$$

Thus a and b commute, but since they were arbitrary we conclude that G is abelian. □

(c) Let p and q be prime numbers (not necessarily distinct), and G a group of order pq. Show that if G is not abelian, then $Z(G) = \{1\}$.

Proof. Since G is not abelian then $Z(G) \neq G$. If $Z(G) \neq 1$ then by Lagrange's theorem, $Z(G)$ has either order p or q. Assume without loss of generality that it has order q. Then $|G/Z(G)| = |G|/|Z(G)| = q$, so that $G/Z(G)$ has prime order and therefore must be cyclic (by TH1#4(a)). But then by part (b) G must be abelian, a contradiction. Therefore $Z(G)$ must be 1. □

3. Let's classify all groups of order 6. To begin, let G be a nonabelian group of order 6. We will show $G \cong S_3$.

(a) Show that there is an element $x \in G$ of order 2. (Once we have Cauchy's theorem for nonabelian groups this part becomes easy, but since G has 6 elements, one can do this by inspection using Lagrange's theorem).

Proof. Since G is not abelian, there is no element of order 6. If there is also no element of order 2, then by Lagrange's theorem, $G = \{1, a, b, c, d, e\}$ where the order of a, b, c, d, e are all 3. Then a^{-1} has order 3 as well, so without loss of generality $a^{-1} = b$, and similarly we may assume $c^{-1} = d$. But this implies that $e^{-1} = e$ contradicting that it has order 3. □

(b) Let $x \in G$ have order 2, and let $H = \langle x\rangle$. Show that H is not normal in G. (*Hint:* Show that if H is normal then $H \leq Z(G)$, then apply 2(c) to find a contradiction.)

Proof. Suppose H is normal, so for all $g \in G$, $gxg^{-1} \in H = \{1, x\}$. If $gxg^{-1} = 1$ then $x = 1$, so we must have $gxg^{-1} = x$. This implies that $x \in Z(G)$ and so $H \leq Z(G)$. But since G is nonabelian of order $6 = 2 \cdot 3$, 2(c) says that its center must be trivial. □

(c) Consider the action of G on $A = G/H$ by left multiplication. Show that the associated permutation representation is injective. Conclude that $G \cong S_3$.

Proof. The action of G on A gives a homomorphism $\varphi : G \to S_A$, and the target (by HW3#7) is isomorphic to S_3. If the action of G on A is faithful, then (by HW3#4), φ is injective, so that we get an injective homomorphism $G \to S_3$, Since they both have order 6, HW1#5 says this has to be an isomorphism. It therefore suffices to show that the action of G on A is faithful.

Let K be the kernel of the action, and suppose that $g \in G$ acts trivially on A. In particular, this means that $g \cdot H = gH = H$, so that $g \in H$. This shows that $K \leq H$. Since H has order 2, this means $K = 1$ or $K = H$. But K is normal, and by part (b), H is not normal, so the only possibility is that $K = 1$, which was our goal. □

(d) Complete the classification of all groups of order 6 by showing that if Z is an abelian group of order 6 then $Z \cong Z_6$. (*Hint:* We do have Cauchy's theorem for abelian groups.) *We've now classified groups of order* ≤ 7.

Proof. By Cauchy's theorem, there are $x, y \in Z$ of order 2 and 3 respectively. We will show that $|xy| = 6$, which gives the result. By Lagrange's theorem, we know $\langle x\rangle \cap \langle y\rangle = 1$. Notice that if $x^i y^j = 1$, then $x^i = y^{-j}$, so that $y^{-j} \in \langle x\rangle$ and so it must be 1, and so $x^i = 1$ as well. In particular, if $(xy)^n = x^n y^n = 1$, then $x^n = y^n = 1$. By HW2#8(c), this means $2|n$ and $3|n$, so that $6|n$. Therefore $|xy| = 6$ as desired. □

4. Let G be a group. Let $[G, G] = \langle x^{-1}y^{-1}xy | x, y \in G\rangle$.

(a) Show that $[G, G]$ is a normal subgroup of G.

Proof. Notice that $[G, G]$ is not the set of elements of the form $x^{-1}y^{-1}xy$, it is the subgroup *generated* by elements of that form. So we need not show it is a subgroup. Lets first prove a lemma.

Lemma 2. *Let H be a group and consider a subset S. To see that $\langle S\rangle$ is normal it suffices to show $hsh^{-1} \in \langle S\rangle$ for all $h \in H$ and $s \in S$.*

Proof. An arbitrary element in $\langle S\rangle$ looks like $s = s_1 s_2 \cdots s_n$ for s_i or s_i^{-1} in S. Then by assumption $gs_ig^{-1} \in \langle S\rangle$, so that:

$$gsg^{-1} = g(s_1s_2\cdots s_n)g^{-1} = (gs_1g^{-1})(gs_2g^{-1})\cdots(gs_ng^{-1}) \in \langle S\rangle.$$

□

Therefore for g and a commutator $x^{-1}y^{-1}xy$, we notice:

$$g(x^{-1}y^{-1}xy)g^{-1} = gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} = (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}),$$

is also a commutator. Therefore the subgroup is normal.

We concluded the proof above, but there is a slightly slicker way to see this, following from the next lemma.

Lemma 3. *Let $\varphi : H \to K$ is a homomorphism of groups. Then the image of a commutator is a commutator.*

Proof. This is immediate, as $\varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y)$. □

Then we need only notice that for every $g \in G$, the conjugation map $\varphi_g : G \to G$ given by $\varphi_g(x) = gxg^{-1}$ is a homomorphism. But we showed this in class: indeed,

$$\varphi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y).$$

Then we immediatly conclude that conjugating a commutator gives a commutator. □

(b) Show that $G/[G,G]$ is abelian.

Proof. We must show that the cosets $xy[G,G]$ and $yx[G,G]$ are equal. But $x^{-1}y^{-1}xy \in [G,G]$ so that

$$xy = yx(x^{-1}y^{-1}xy) \in yx[G,G].$$

Since the cosets form a partition, we are done. □

$[G,G]$ is called the *commutator subgroup* of G, and $G/[G,G]$ is called the *abelianization* of G, denoted G^{ab}. The rest of this exercise explains why.

(c) Let $\varphi : G \to H$ be a homomorhism with H abelian. Show $[G,G] \subseteq \ker\varphi$.

Proof. It suffices to show that every element $x^{-1}y^{-1}xy \in G$ is in the kernel of φ, since then $[G,G]$ is generated by elements in the kernel. But then:

$$\varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y) = \varphi(x)\varphi(x)^{-1}\varphi(y)^{-1}\varphi(y) = 1,$$

as H is abelian. (Notice we also just showed that the commutator subgroup of an abelian group is always the trivial subgroup). □

(d) Conclude that for H an abelian group there is a bijection:

$$\left\{ \text{ Homomorphisms } \varphi : G \to H \ \right\} \Longleftrightarrow \left\{ \text{ Homomorphisms } \tilde{\varphi} : G^{\mathrm{ab}} \to H \ \right\}$$

Hint. *Recall the technique of passing to the quotient described at the beginning of the 2/23 lecture*

Proof. We remind the reader of the statement of “Passing to the Quotient.”

Lemma 4 (Passing to the Quotient)**.** *Let $N \trianglelefteq G$ be a normal subgroup, and $\varphi : G \to H$ a homomorphism. If $N \leq \ker\varphi$, then there is a unique homomorphism $\tilde{\varphi} : G/N \to H$ such that $\tilde{\varphi} \circ \pi = \varphi$, defined by the rule $\tilde{\varphi}(gN) = \varphi(g)$. This is summarized by the following diagram.*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & H \\ G/N. \arrow[ur, dotted, "\tilde{\varphi}"'] & \end{tikzcd}$$

With this lemma we prove part (d). In the righthand direction we define a function Φ which takes a map $\varphi : G \to H$ to the unique map $\tilde{\varphi}$ from the lemma, which exists because $[G, G] \leq \ker \varphi$ by part (c). In the other direction define Ψ which takes a map $\tilde{\varphi}$ to the composition $\varphi = \tilde{\varphi} \circ \pi$:

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[rr, bend left, "\varphi"] & G^{\text{ab}} \arrow[r, "\tilde{\varphi}"] & H. \end{tikzcd}$$

We must prove these processes are inverses to eachother. But this is obvious. $\Psi \circ \Phi(\varphi) = \tilde{\varphi} \circ \pi = \varphi$ by definition, and $\Phi \circ \Psi(\tilde{\varphi}) = \Phi(\tilde{\varphi} \circ \pi) = \tilde{\varphi}$ by the uniqueness of $\tilde{\varphi}$.
We make a remark that this is a sort of *universal property*, in that G^{ab} is the universal abelianization of G. I won't get into precisely what this means at the moment, but it can be understood via the slogan: Maps from G to abelian things are the same as maps from G^{ab} to abelian things. □

5. Let's now compute D_{2n}^{ab}. We should begin computing $xyx^{-1}y^{-1}$. There are 3 cases.

   (a) Compute $x^{-1}y^{-1}xy$ in each of the following 3 cases. (*Hint:* HW2#9(e) gives the inverse for a reflection.)

   (i) x, y both reflections. So $x = sr^i$ and $y = sr^j$.

   Proof. Since reflections always have order two, we have $x^{-1} = x$ and $y^{-1} = y$. That is:
   $$x^{-1}y^{-1}xy = (sr^i)(sr^j)(sr^i)(sr^j) = r^{j-i}r^{j-i} = r^{2(j-i)}$$
   As i and j vary we collect all even powers of r. □

   (ii) x a reflection and y not a reflection. So $x = sr^i$ and $y = r^j$.

   Proof. In this case $x^{-1} = x$, but that is not true for y. We computeL
   $$x^{-1}y^{-1}xy = (sr^i)(r^{-j})(sr^i)(r^j) = (sr^{i-j})(sr^{i+j}) = r^{2j},$$
   and as above we collect precisely the even powers of r. □

   (iii) Neither x nor y are reflections. So $x = r^i$ and $y = r^j$.

   Proof. Here x and y commute so their commutator is 1. □

   (b) Prove that $[D_{2n}, D_{2n}] = \langle r^2 \rangle$. If n is odd one could choose another generator. What is it?

   Proof. We saw in part (a) that the commutators of D_{2n} are precisely the even powers of r, proving the first statement. If n is odd, then $(n+1)/2$ is an integer and we can compute
   $$(r^2)^{(n+1)/2} = r^{n+1} = r,$$
   so that in fact the commutator subgroup is $\langle r \rangle$. □

   (c) Now prove that D_{2n}^{ab} is either V_4 or Z_2 depending on whether n is odd or even. Note that since this is so small we should interpret this as suggesting that D_{2n} is far from abelian.

Proof. Note that:

$$|D_{2n}^{\text{ab}}| = |D_{2n}/|[D_{2n}, D_{2n}]| = |D_{2n}|/|[D_{2n}, D_{2n}]|.$$

If n is odd, then $|[D_{2n}, D_{2n}]| = n$ which is half the order of D_{2n}. Thus $|D_{2n}^{\text{ab}}| = 2$, and so it must be Z_2 by TH1#4(a).

If n is even then $|[D_{2n}, D_{2n}]| = n/2$, a quarter of the order of D_{2n}, and so $|D_{2n}^{\text{ab}}| = 4$ so it must be Z_4 or V_4 by TH1#4(d). To see it is V_4 we will show every element has order 2. The cosets are represented by r, s, and sr. The latter two have order two already in D_{2n}, so it remains to show that the coset represented by r does too, but its square is r^2 which generates the commutator subgroup. Since every element of D_{2n}^{ab} has order 2, it must be the group V_4. □

For the remainder we will study the quaternion group Q_8. It is a nonabelian group with very interesting properties.

Definition 1. *The quaternion group of order 8, denoted Q_8 is the group of the following 8 elements:*

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

subject to the relations:

$$(-1)^2 = 1$$
$$i^2 = j^2 = k^2 = -1,$$
$$(-1)x = -x = x(-1) \text{ for all } x,$$

$$\begin{aligned} ij &= k, & ji &= -k, \\ jk &= i, & kj &= -i, \\ ki &= j, & ik &= -j. \end{aligned}$$

6. Let's start with a few simple facts. Much of this is worked out in the book.

   (a) Write the entire multiplication table for Q_8.

   Proof. The group is nonabelian, so we make sure to stick to the convention that in row a and column b we are writing ab (rather than ba),

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

□

(b) Find 2 elements which generate all of Q_8. (*Bonus:* Can you give a presentation of Q_8?)

Proof. Notice that i and j generate everything. Indeed:

$$\begin{array}{ccc} -1 = i^2 & -i = i^3 & -j = j^3 \\ 1 = i^4 & k = ij & -k = ji. \end{array}$$

The following is an intuitive presentation, but I want to point out that -1 is tacitly a generator here:

$$\langle i, j \mid i^2 = j^2 = -1, ij = -ji \rangle.$$

This answer is acceptable on this assignment, but not precisely correct. We probably want to assume in our presentation that we don't know what -1 is (i.e., that its square is 1). The correct presentation, that doesn't include -1 secretly is:

$$\langle i, j \mid i^4 = j^4 = 1,\ i^2 = j^2 \text{ and } ji = i^3 j \rangle.$$

Where translating back to the more intuitive notation $i^2 = j^2 = -1$, $ij = k$, and $ji = i^3 j = (i^2) ij = -k$. $\square$

(c) Prove that Q_8 is not isomorphic to D_8.

Proof. The easiest way to see this is to notice that if they were isomorphic, they would need to have the same number of elements of order n for each n. Then we can consider the order of every element in each group.

Q_8	order		D_8	order
1	1		1	1
-1	2		r	4
i	4		r^2	2
$-i$	4		r^3	4
j	4		s	2
$-j$	4		sr	2
k	4		sr^2	2
$-k$	4		sr^3	2

In particular, Q_8 only has one element of order 2 whereas D_8 has 5. $\square$

(d) Find all the subgroups of Q_8, and draw its lattice. (*Hint*: there are 6 total subgroups).

Proof. The nontrivial subgroups (i.e., those which aren't Q_8 and $\{1\}$) must have orders 2 or 4 by Lagranges theorem. The order 2 subgroups must be cyclic, generated by an element of order 2. The only element of order 2 is -1, so the only subgroup of order 2 is $\{\pm 1\}$. As for subgroups of order four, they are either cyclic or isomorphic to the Klein 4 group V_4. But V_4 must be generated by 2 elements of order 2, and Q_8 only has one. Thus each subgroup of order 4 is cyclic. There are 6 elements of order 4, but $-i = i^3$, and similarly for j and k, so there 3 subgroups of order 4 generated by i and j and k.

As $i^2 = j^2 = k^2 = -1$, the subgroup $\{\pm 1\}$ is contained in all of them. thus the lattice is as follows.

$$\begin{tikzcd}[column sep=small]
 & Q_8 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle i \rangle \arrow[dr, dash] & \langle j \rangle \arrow[d, dash] & \langle k \rangle \arrow[dl, dash] \\
 & \{\pm 1\} \arrow[d, dash] & \\
 & \{1\} &
\end{tikzcd}$$

□

(e) Prove that every subgroup of Q_8 is normal.

Proof. Q_8 and $\{1\}$ are automatically normal. Next notice that since $-1 * a = a * -1$ for each $a \in Q_8$. Thus $\{\pm 1\}$ is contained in the center of Q_8 and is therefore normal by 2(a) above.

The cases for $\langle i \rangle, \langle j \rangle$ and $\langle k \rangle$ are completely symmetric, so we just treat the case of $H = \langle i \rangle$. Notice that

$$H \leq N_{Q_8}(H) \leq Q_8.$$

Also $|H| = 4$ and $|N_{Q_8}(H)|$ divides 8 by Lagrange's theorem, so that $N_{Q_8}(H)$ is either H or all of Q_8. Thus if we exhibit one element of the normalizer which is not in H, the normalizer is all of Q_8, which precisely means that $H \trianglelefteq Q_8$. Notice that:

$$jij^{-1} = ji(-j) = (-k)(-j) = kj = -i \in \langle i \rangle.$$

Thus $j \in N_{D_8}(H)$ and we are done. □

(f) Prove that every *proper* subgroup and quotient group of Q_8 is abelian (*Hint*: TH1#4).

Proof. Let H be a proper subgroup or quotient of Q_8. Then by Lagrange's theorem, $|H| = 1, 2$ or 4. In the first case H is the trivial group which is abelian, in the second it is isomorphic to Z_2 which is abelian, and in the third it is isomorphic to either Z_4 or V_4 which are abelian. □

(g) Compute $Z(Q_8)$ and $Q_8/Z(Q_8)$ (*Hint for the second part*: you can do this by hand, but it might be slicker to apply 2(b)).

Proof. It is readily checked using the multiplication table in part (a) that $Z(Q_8) = \{\pm 1\}$. Then

$$|Q_8/Z(Q_8)| = |Q_8|/|\{\pm 1\}| = 8/2 = 4.$$

Then in particular, it is either cyclic or isomorphic to V_4. If it is cyclic, then 2(b) says that Q_8 is abelian, which is false. So the quotient is V_4. (Note, one could also use the lattice from part (d) together with the fourth isomorphism theorem to see that the lattice of the quotient has to be the lattice above $\{\pm 1\}$, which is the lattice of V_4). □

7. Now let's follow the proof of Cayley's theorem to exhibit Q_8 as a subgroup of S_8.

   (a) Label $\{1, -1, i, -i, j, -j, k, -k\}$ as the numbers $\{1, 2, \cdots, 8\}$. Then the action of Q_8 on itself by left multiplication gives an injective map $Q_8 \to S_8$. Write the permutation representations for -1 and i as elements $\sigma_{-1}, \sigma_i \in S_8$, and verify that $\sigma_i^2 = \sigma_{-1}$. (Using the multiplication table from question 1 will make this easier).

   Proof. Let's first compute σ_{-1}.

$$\begin{array}{rcl}
-1 * 1 = -1 & \leftrightarrow & \sigma_{-1}(1) = 2 \\
-1 * -1 = 1 & \leftrightarrow & \sigma_{-1}(2) = 1 \\
-1 * i = -i & \leftrightarrow & \sigma_{-1}(3) = 4 \\
-1 * -i = i & \leftrightarrow & \sigma_{-1}(4) = 3 \\
-1 * j = -j & \leftrightarrow & \sigma_{-1}(5) = 6 \\
-1 * -j = j & \leftrightarrow & \sigma_{-1}(6) = 5 \\
-1 * k = -k & \leftrightarrow & \sigma_{-1}(7) = 8 \\
-1 * -k = k & \leftrightarrow & \sigma_{-1}(8) = 7
\end{array}$$

   Thus σ_{-1} swaps 1 and 2, 3 and 4, 5 and 6, 7 and 8. That is:

$$\sigma_{-1} = (12)(34)(56)(78) \in S_8.$$

   Let's do a similar computation for σ_i.

$$\begin{array}{rcl}
i * 1 = i & \leftrightarrow & \sigma_i(1) = 3 \\
i * -1 = -i & \leftrightarrow & \sigma_i(2) = 4 \\
i * i = -1 & \leftrightarrow & \sigma_i(3) = 2 \\
i * -i = 1 & \leftrightarrow & \sigma_i(4) = 1 \\
i * j = k & \leftrightarrow & \sigma_i(5) = 7 \\
i * -j = -k & \leftrightarrow & \sigma_i(6) = 8 \\
i * k = -j & \leftrightarrow & \sigma_i(7) = 6 \\
i * -k = j & \leftrightarrow & \sigma_i(8) = 5
\end{array}$$

   Thus σ_i takes 1 to 3 to 2 to 4 to 1, while taking 5 to 7 to 6 to 8 and back to 5. Thus we have:

$$\sigma_i = (1324)(5768) \in S_8.$$

   Next we compute the square of σ_i by hand, using in the first equality that disjoint cycles commute.

$$\begin{aligned}
(\sigma_i)^2 &= (1324)^2(5768)^2 \\
&= (1324)(1324)(5768)(5768) \\
&= (12)(34)(56)(78).
\end{aligned}$$

   □

   (b) Use the generators from question 6(b) to give two elements of S_8 which generate a subgroup $H \leq S_8$ isomorphic to Q_8.

Proof. Since i and j generate Q_8, the permutations σ_i and σ_j generate the isomorphic subgroup of S_8. Thus we must also compute σ_j like we did for i and -1 in part (a).

$$\begin{array}{ccc} j*1=j & \leftrightarrow & \sigma_j(1)=5 \\ j*-1=-j & \leftrightarrow & \sigma_j(2)=6 \\ j*i=-k & \leftrightarrow & \sigma_j(3)=8 \\ j*-i=k & \leftrightarrow & \sigma_j(4)=7 \\ j*j=-1 & \leftrightarrow & \sigma_j(5)=2 \\ j*-j=1 & \leftrightarrow & \sigma_j(6)=1 \\ j*k=i & \leftrightarrow & \sigma_j(7)=3 \\ j*-k=-i & \leftrightarrow & \sigma_j(8)=4 \end{array}$$

Therefore we get:

$$\sigma_j = (1526)(3847).$$

Thus we have:

$$Q_8 \cong \langle \sigma_i, \sigma_j \rangle = \langle (1324)(5768), (1526)(3847) \rangle \leq S_8.$$

□

(c) Is σ_i even or odd?

Proof. Let's compute the sign. We use the fact that the sign of an m-cycle is even if and only if m is odd. Then,

$$\epsilon((1324)(5768)) = \epsilon((1324))\epsilon((5768)) = (1)(1) = 1.$$

Thus σ_i is even. □

(d) $A_8 \cap H$ is isomorphic to a subgroup of Q_8. Which one?

Proof. As in part (c) one can easily compute that σ_j is even as well, so that the entire subgroup they generate is contained in A_8. Thus $A_8 \cap H = H \cong Q_8$. □

8. Cayley's theorem says that if $|G| = n$ then G embeds at S_n. One could ask if this n is *sharp*, or if perhaps G can embed in some smaller symmetric group. For example, D_8 embeds in S_4 (thinking about symmetries of the square as permutations of the vertices, cf HW3#5). Nevertheless, for Q_8 the symmetric group given by Cayley's theorem is the smallest.

(a) Let Q_8 act on a set A with $|A| \leq 7$. Let $a \in A$. Show that the stabilizer of a, $(Q_8)_a \leq Q_8$ must contain the subgroup $\{\pm 1\}$. (*Hint:* The orbit stabilizer theorem might help.)

Proof. Let $a \in A$, and denote the stabilizer of a by the subgroup $(Q_8)_a \leq Q_8$. Then recall that the index of the stabilizer of a is Q_8 is the same as the size of the orbit of a $Q_8 \cdot a$ which is a subset of A. That is:

$$|Q_8 : (Q_8)_a| = |Q_8 \cdot a| \leq |A| \leq 7 < 8.$$

The left hand size is $8/|(Q_8)_a|$ by Lagrange's theorem, so that $(Q_8)_a$ cannot be the trivial subgroup of Q_8. But in the lattice from 1(d), we saw that every nontrivial subgroup of Q_8 contains $\{\pm 1\}$, completing the proof. □

(b) Deduce that the kernel of the action of Q_8 on A contains $\{\pm 1\}$.

Proof. $\{\pm 1\}$ is contained in the stabilizer of every element of A by part (a), and so it acts trivially on all of A. This is precisely what it means to be in the kernel. □

(c) Conclude that Q_8 cannot embed into S_n for $n \leq 7$. That is, show there is no injective homomorphisms $Q_8 \hookrightarrow S_n$ for $n \leq 7$.

Proof. By HW3#4, an embedding $Q_8 \hookrightarrow S_n$ corresponds to a faithful action on the set $\{1, 2, \cdots, n\}$. But we just saw that if $n \leq 7$, any action on $\{1, 2, \cdots, n\}$ has a nontrivial kernel. □