MATH 31 – HOMEWORK 3 SOLUTIONS!

due Wednesday, July 19

Instructions: This assignment is due at the *beginning* of class. Staple your work together (do not just fold over the corner). Please write the questions in the correct order. If I cannot read your handwriting, you won't receive full credit.

1. (*6 points*) (6.12) Let G and H be finite groups. Show that if $G \times H$ is cyclic, then (i) G and H are cyclic, and (ii) every subgroup of $G \times H$ is of the form $A \times B$ for some subgroups A and B of G and H, respectively.

   Solution: Assume that G and H are finite groups and that $G \times H$ is cyclic. Our first goal is to prove that G and H are cyclic.

   To start with, we should figure out what we can learn from our assumptions. As $G \times H$ is cyclic, it is generated by some element. In other words, there exists an element $(g,h) \in G \times H$ such that

   $$G \times H = \langle (g,h) \rangle.$$

   Our first goal is to show that G and H are cyclic. One way to show that a group is cyclic is to find an element that you think is a generator, and then prove that it is. Can't figure out a good candidate for generators for G and H? Try an example first. We know that $\mathbb{Z}_3 \times \mathbb{Z}_4$ is cyclic—what are its generators? What are the generators of $\mathbb{Z}_3$ and of $\mathbb{Z}_4$ on their own? Does something jump out at you?

   Given that (g,h) is a generator for $G \times H$, it's reasonable to ponder whether g is a generator for G and h is a generator for H. So, now we will make that claim, then try to prove it.

   Claim: $G = \langle g \rangle$ and $H = \langle h \rangle$.
   Proof of claim: To show that $G = \langle g \rangle$, we need to show that every element in G is some power of g. Let $a \in G$. Because we already know that (g,h) is a generator for $G \times H$, every element of $G \times H$ is a power of (g,h). One of these elements is (a, e_H). This tells us that there exists an integer m such that

   $$(a, e_H) = (g,h)^m = (g^m, h^m).$$

   Therefore, $a = g^m$. As a was chosen arbitrarily, we've proved that every element of G is a power of g. This proves that $G = \langle g \rangle$, and hence that G is cyclic. An almost identical argument proves that H is cyclic, and therefore the claim is proved.

   Part (ii) asks us to show that every subgroup of $G \times H$ has the form $A \times B$ for some $A \leq G$ and $B \leq H$. To prove this, pick an arbitrary subgroup $S \leq G \times H$. We've learned that every subgroup of a cyclic group is itself cyclic, and moreover is generated by a power of the generator of the whole group. Hence, there exists an integer m such that

   $$S = \langle (g,h)^m \rangle = \langle (g^m, h^m) \rangle.$$

   To show that S has the form $A \times B$, we'll try to figure out first what A and B might be, then prove that it works. (Again, if you get stuck, try with some examples. We know it should work for $\mathbb{Z}_3 \times \mathbb{Z}_4$ but not $\mathbb{Z}_2 \times \mathbb{Z}_2$.)

   Claim: $S = A \times B$ where $A = \langle g^m \rangle$ and $B = \langle h^m \rangle$.
   Proof of claim: The elements of S are powers of $(g,h)^m$. In other words,

   $$S = \{((g,h)^m)^k : k \in \mathbb{Z}\} = \{(g^{mk}, h^{mk}) : k \in \mathbb{Z}\}.$$

On the other hand
$$A \times B = \{(g^{mi}, h^{mj}) : i, j \in \mathbb{Z}\}.$$

From this we see immediately that $S \subseteq A \times B$. At first it would appear that $A \times B$ is much bigger than S, but our assumption that $G \times H$ is cyclic will allow us to show that this is not the case. Pick an arbitrary element $(g^{mi}, h^{mj}) \in A \times B$. Since $G \times H = \langle (g, h) \rangle$, there exists an integer ℓ such that

$$(g, h)^{\ell} = (g^i, h^j),$$

and therefore
$$(g^{mi}, h^{mj}) = (g^i, h^j)^m = (g, h)^{\ell m} = ((g, h)^m)^{\ell} \in S.$$

Therefore, $A \times B \subseteq S$, proving that actually $S = A \times B$. As S was an arbitrarily chosen subset, we've now proved that all subsets of $G \times H$ have the required form. □

---

2. (*6 points*) (6.13) Prove the converse of the result in the previous question. That is, show that for finite groups G and H, (i) and (ii) of the previous question (taken together) imply that $G \times H$ is cyclic.

Solution: Assume that G and H are finite cyclic groups, and that every subgroup of $G \times H$ has the form $A \times B$ where $A \leq G$ and $B \leq H$. We aim to prove that $G \times H$ is also cyclic.

First, we use the assumption that G and H are cyclic to conclude that there exist $g \in G$ and $h \in H$ such that $G = \langle g \rangle$ and $H = \langle h \rangle$. In order to prove that $G \times H$ is cyclic, we will produce a generator.

Claim: $G \times H = \langle (g, h) \rangle$.
Proof of claim: We don't know yet if $\langle (g, h) \rangle = G \times H$ but it's definitely at least a subset of $G \times H$. Therefore, by our assumption, there exists a subgroup A of G and a subgroup B of H such that

$$\langle (g, h) \rangle = A \times B.$$

As a set, what elements are in $A \times B$? By the definition of the direct product,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

Since the element (g, h) is in $A \times B$, it must be true that $g \in A$ and $h \in B$. But, as g is a generator for G and h is a generator for H, this is only possible if $A = G$ and $B = H$, proving that

$$\langle (g, h) \rangle = G \times H$$

and hence that $G \times H$ is cyclic. □

---

3. (*4 points*) Write each permutation as a product of disjoint cycles, then as a product of transpositions. Determine whether each permutation is even or odd.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 5 & 6 & 4 & 2 & 8 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 2 & 3 & 7 & 4 & 5 & 6 \end{pmatrix}$

Solution: For each permutation, we first convert it from two-line notation to cycle notation, and then from cycle notation to a product of transpositions.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix} = (\,1\,2\,4\,)(\,3\,6\,5\,) = (\,1\,4\,)(\,1\,2\,)(\,3\,5\,)(\,3\,6\,)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix} = (\,1\,6\,3\,4\,)(\,2\,5\,) = (\,1\,4\,)(\,1\,3\,)(\,1\,6\,)(\,2\,5\,)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 1 & 5 & 6 & 4 & 2 & 8 \end{pmatrix} = (\,1\,3\,)(\,2\,7\,)(\,4\,5\,6\,)(\,8\,) = (\,1\,3\,)(\,2\,7\,)(\,4\,6\,)(\,4\,5\,)(\,1\,8\,)(\,1\,8\,)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 2 & 3 & 7 & 4 & 5 & 6 \end{pmatrix} = (\,1\,8\,6\,4\,3\,2\,)(\,5\,7\,) = (\,1\,2\,)(\,1\,3\,)(\,1\,4\,)(\,1\,6\,)(\,1\,8\,)(\,5\,7\,)$$

These are all even.

---

4. (*4 points*) (8.7) Prove that S_n is nonabelian if $n \geq 3$.

   Solution: Let $n \geq 3$ and consider the following two permutations of length n: $(\,1\;2\,)$ and $(\,1\;3\,)$. Of course, these really mean

   $$(\,1\,2\,)(\,3\,)(\,4\,)\cdots(\,n\,) \qquad \text{and} \qquad (\,1\,3\,)(\,2\,)(\,4\,)\cdots(\,n\,).$$

   Since $(\,1\;2\,)(\,1\;3\,) = (\,1\;3\;2\,)$ and $(\,1\;3\,)(\,1\;2\,) = (\,1\;2\;3\,)$, we see that S_n is nonabeliean if $n \geq 3$. □
