Math 132H Homework 1

Thomas Slavonia; UID: 205511702

April 9, 2024

1.

We begin by noting that $|S_3| = 3!$, so apart from ϕ and ψ, we need to find four more elements of S_3 by taking the compositions of ϕ and ψ.

$$\phi \circ \phi = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$$
$$\psi \circ \psi = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$
$$\phi \circ \psi = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$$
$$\psi \circ \phi = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

2.

Proof. Let G and H be groups with operations $*$ and $\cdot$ respectively and G and/or H nonabelian. Define the operation of the group $G \times H$ as

$$(g, h) \circ (g', h') = (g * g', h \cdot h').$$

We showed in lecture that $G \times H$ is indeed a group. Also, the group $G \times H$ is also nonabelian, as if either $g * g' \neq g' * g$ or $h \cdot h' \neq h' \cdot h$, then

$$(g, h) \circ (g', h') = (g * g', h \cdot h') \neq (g' * g, h' \cdot h) = (g', h') \circ (g, h).$$

We must show that $|G \times H| = |G||H|$. To show this, we can note that for the first component of any element of $G \times H$, we have $|G|$ choices, and similarly, for the second component, we have $|H|$. Thus, we have that $|G \times H| = |G||H|$. We know from the textbook that D_4 is a nonabelian group; therefore, $D_4 \times D_4$ is a nonabelian group of order 16. Similarly, using that $G \times H$ is nonabelian if either G or H is nonabelian, we can define $D_4 \times \mathbb{Z}_6$ is a nonabelian group of order 48. Lastly, note that $D_3 = \{r_0, r_1, r_2, s, t, u\}$ is nonabelian as $r_1 s \neq s r_1$ (further visualization in the book), so we have $D_3 \times \mathbb{Z}_2$ and $D_4 \times \mathbb{Z}_5$ as nonabelian groups of order 12 and 30 respectively.

□

3.

a.

Proof. Let $a \in G$ and suppose $|a| = 12$. Let $n = 12 = |a|$. We will apply the theorem that states that if $n = td$ for $d \geq 1$, then a^t has order d repeatedly throughout this problem. The theorem applies to the following:

$$12 = 1 \cdot 12 \Rightarrow |a| = 12$$
$$12 = 2 \cdot 6 \Rightarrow |a^2| = 6$$
$$12 = 3 \cdot 4 \Rightarrow |a^3| = 4$$
$$12 = 4 \cdot 3 \Rightarrow |a^4| = 3$$
$$12 = 6 \cdot 2 \Rightarrow |a^6| = 2.$$

We now know that $|a^3| = 6$ and that $(a^3)^3 = a^9$. Note that $a^k = e$ if and only if $n|k$, thus, $a^{12} = e$, $a^{24} = e$, $a^36 = e$, $a^{48} = e$, $a^{60} = e$, $a^{84} = e$, and $a^{132} = e$. Thus, the least common multiples of n and $5, 7, 8, 9, 10, 11$ and 12 are $60, 84, 24, 36, 60, 132$ respectively. Now, we know that $a^{60} = \left(a^5\right)^{12}$, $a^{84} = \left(a^7\right)^{12}$, $a^{24} = \left(a^8\right)^3$, $a^{36} = \left(a^9\right)^4$, $a^{60} = \left(a^{10}\right)^6$, and $a^{132} = \left(a^{11}\right)^{12}$. This all implies that $|a^5| = 12$, $|a^7| = 12$, $|a^8| = 3$, $|a^9| = 4$, $|a^{10}| = 6$, and $|a^{11}| = 12$. □

b.

Proof. My conjecture on the order of a^k when $|a| = n$ is that is the order of $|a^k| = \frac{n}{gcd(k,n)}$. □

4.

Proof. Let $G = \{a_1, a_2, \ldots, a_n\}$ be a finite abelian group of order n. Let $x = a_1 a_2 \cdots a_n$. Thus, $x^2 = a_1 a_2 \cdots a_n a_1 a_2 \cdots a_n$. Every element of a group must have an inverse; therefore, a_i^{-1} is represented somewhere in the product $a_1 a_2 \cdots a_n$. Because the group is commutative, we can commute the elements of the sum (which are all elements of the group) to get that $a_1 a_2 \cdots a_n = a_1^{-1} a_2^{-1} \cdots a_n^{-1}$. Now, $x^2 = a_1 a_2 \cdots a_n a_1^{-1} a_2^{-1} \cdots a_n^{-1}$ which we can once again use the commutative of the group to rewrite this as $x^2 = a_1 a_1^{-1} a_2 a_2^{-1} \cdots a_n a_n^{-1} = e$. □

5.

Proof. Suppose G is a group where every nonidentity element has order 2. Take $a, b \in G$. We want to show that $ab = ba$. Using our assumption, we find

$$e = a^2 = aa = aea = ab^2a = abba$$

which implies

$$a^{-1}b^{-1} = ab$$

and thus

$$a^{-1} = abb = ab^2 = ae = a.$$

Note that every element of a group has a unique inverse and is closed under multiplication; hence, for $ab \in G$, $(ab)^{-1} = b^{-1}a^{-1}$ as $abb^{-1}a^{-1} = e$. We also now know that every element of the group is equal to its inverse. Therefore, we can conclude that $ab = b^{-1}a^{-1}$, $a = a^{-1}$, and $b = b^{-1}$ and get the desired result:

$$ab = b^{-1}a^{-1} = ba.$$

□

6.

Proof. Suppose, for a group G, that $(ab)^i = a^i b^i$ for three consecutive integers i and every $a, b \in G$. Take $a, b \in G$. Also, without loss of generality, suppose the consecutive integers are i, $i+1$, and $i+2$. We use these properties to see

$$a^{i+1}b^{i+1} = (ab)^{i+1} = ab(ab)^i = aba^ib^i$$

which implies that

$$a^{i+1}b = aba^i$$

and by multiplying on the right by a^{-1} we get

$$a^ib = ba^i.$$

Similarly,

$$a^{i+2}b^{i+2} = (ab)^{i+2} = ab(ab)^{i+1} = aba^{i+1}b^{i+1}.$$

which implies

$$a^{i+1}b = ba^{i+1}.$$

Thus, we can find

$$ab = aba^ia^{-i} = aa^iba^{-i} = a^{i+1}ba^{-i} = ba^{i+1}a^{-i} = ba.$$

□