MTH 320 - Abstract Algebra

HW #3 Solutions

October 14th, 2020

Question 1: Let $(D, \cdot)$ be a group with 130 elements. Given $a, b \in D$ such that $a \cdot b = b \cdot a$, $|a| = 10$ and $|b| = 13$, prove that D is an Abelian group. What more can we say about this group?

We are given some $a, b \in D$ such that $|a| = 10$ and $|b| = 13$. By previous result shown in HW1, we know that since $(D, \cdot)$ is a group and we have two elements in D, say a and b, then $|a \cdot b| = |a| \cdot |b|$ if $\gcd(|a|, |b|) = 1$ and $a \cdot b = b \cdot a$.

In our case, we know that $\gcd(10, 13) = 1$, meaning that for some $c = a \cdot b \in D$, $|c| = |a| \cdot |b| = 10 \cdot 13 = 130$. This means that the order of the element c is 130, or in other words, there exists an element inside D such that the order of the element is equal to the cardinality of D itself. Mathematically:

$$\exists c \in D \text{ st } |c| = 130 = |D|$$

With this knowledge, we know that c forms up the entirety of the group, D. In other words, $D = <c>$. Every other element in the group, $(D, \cdot)$ can be made by taking c to some power, where the power represents the repitition of the binary operation, $(\cdot)$.

This means that D is indeed not only a group, but a *cyclic* group. Automatically, through the discussion introduced in class, we know that if a group is cyclic, then it is also Abelian. Therefore we have proven that $(D, \cdot)$ is Abelian, and went an extra step to show that it is alo cyclic.

Question 2:

i. Assume $(D, \cdot)$ is an infinite cyclic group and $a \in D$ st $a \neq e$. Prove that $|a| = \infty$.

   Since $(D, \cdot)$ is an infinite cyclic group, $D = <a>$ for some $a \in D$. Let $b \in D$ and assume that $|b| = m$. Since we know that $b \in D = <a>$, then we conclude that $b = a^k$ for some $k \in \mathbb{Z}$.

   Since $|b| = m$, we have that $b^m = e$, which means that $(a^k)^m = e$. However, this is a contradiction because we are saying that a^{km}, where km is a <u>finite</u> number gives us the identity, e. Since $(D, \cdot)$ is an infinite cyclic group, we conclude that $|a| = \infty$.

ii. We know that $(\mathbb{Z}_8, +)$ is cyclic and $(\mathbb{Z}, +)$ is cyclic. Prove that $\mathbb{Z}_8 \oplus \mathbb{Z}$ is not a cyclic group. Use the above proof from (i).

   Let $x = (1, 0) \in \mathbb{Z}_8 \oplus \mathbb{Z}$. Then we know that $|x| = \text{lcm}(|1|, |0|) = \text{lcm}(8, 1) = 8$. Since x is not the identity of $\mathbb{Z}_8 \oplus \mathbb{Z}$ by our choice, and it is of finite order, we can conclude using (i) that D is NOT cyclic.

iii. Let $(H, \cdot)$ and $(K, *)$ be cyclic groups st $|H| = m$ and $|K| = n$. Let $D = H \oplus K$. Prove that D is cyclic iff $\gcd(m, n) = 1$.

$$\Longrightarrow$$

$$\text{Assume } D \text{ is cyclic, show } \gcd(m,n) = 1$$
$$\text{let } h \in H, k \in K$$

$$\text{We know that since } D = H \oplus K, \text{ then } |D| = |H| \times |K|$$
$$\text{ie } |D| = m\,n$$

$$\text{Since } H \text{ is cyclic, it has exactly } \varphi(m) \text{ elements of order } m$$
$$\text{Similarly, } K \text{ has exactly } \varphi(n) \text{ elements of order } n$$
$$\text{(From class result)}$$

$$\text{We are assuming that } D \text{ is cyclic, ie } \exists a \in D \text{ st } |a| = |D| \qquad a = (h, k)$$
$$|a| = |(h,k)| = m \times n$$
$$\text{We know that the concept of order suggests the LEAST}$$
$$\text{positive number st } a^{m \times n} = e, \text{ leading us to the fact that:}$$
$$\operatorname{lcm}(m,n) = m \times n$$

$$\gcd(m,n) = \frac{m \times n}{\operatorname{lcm}(m,n)} = \frac{m\,n}{m\,n} = 1$$

$$\Longleftarrow$$

$$\text{Assume } \gcd(m,n) = 1, \text{ show that } D \text{ is cyclic}$$
$$\gcd(m,n) = \frac{m\,n}{\operatorname{lcd}(m,n)} \Rightarrow \operatorname{lcd}(m,n) = m\,n$$

$$\text{Let } h \in H \text{ and } k \in K$$
$$\text{Since } H \text{ and } K \text{ are both cyclic groups, then } \exists h \in H \text{ st } |h| = m = |H|$$
$$\text{and similarly, } \exists k \in K \text{ st } |k| = n = |K|$$

$$|D| = m\,n \text{ (By previous proof)}$$

$$\text{Let } a = (h,k) \in D$$
$$|a| = \operatorname{lcm}(m,n) \qquad \text{By definition of } D$$
$$|a| = n\,m$$

$$\text{Therefore, } \exists a \in D \text{ st } |a| = |D| = |H| \times |K| = m\,n$$
$$\text{And hence } D \text{ is cyclic, } D = <a>$$

iv. Let $D = (\mathbb{Z}_8, +) \oplus (\mathbb{Z}_{15}, +)$. Then, by (iii), D is cyclic. How many generators does D have? Find all subgroups of D with 20 elements. How many elements of order 40 does D have?

Since $\gcd(8, 15) = 1$, D is cyclic and $|D| = |\mathbb{Z}_8| \times |\mathbb{Z}_{15}|$. We know that $\mathbb{Z}_8$ has $\varphi(8) = 4$ generators and similarly, $\mathbb{Z}_{15}$ has $\varphi(15) = 8$ generators. This means that the number of generators for D is exactly $4 \times 8 = 32$, since each pair of two generators from $\mathbb{Z}_8$ and $\mathbb{Z}_{15}$ can form a generator for D.

We know that $|D| = 15 \times 8 = 120$. This means that the total number of elements in D is 120. By a class result, we know that since $20|120$, then there exists a unique subgroup of D where the cardinality is 20. In other words, this subgroup contains exactly 20 elements, and it is the only one that does.

There is exactly one subgroup, H, of D with 20 elements. Choose one element in D with order 20. For example, choose $x = (2, 3)$. $|x| = 20$. Thus $H = <(2, 3)> = F \oplus K$, where $F = \{0, 2, 4, 6\} < \mathbb{Z}_8$ (subgroup of $\mathbb{Z}_8$) and $K = \{0, 3, 6, 9, 12\} < \mathbb{Z}_{15}$ (subgroup of $\mathbb{Z}_{15}$).

To find the number of elements in D that have order 40, we consider the following:

$$\begin{aligned}
&\text{Let } d = (h, k) \in D\\
&h \in \mathbb{Z}_8, k \in \mathbb{Z}_{15}\\
&\text{st lcm}\,(|h|, |k|) = 40 \quad \forall d \in D\\
\\
&|h| = 8, |k| = 5 \text{ or } |h| = 5, |k| = 8\\
&\text{In either case,}\\
&\text{the number of elements with order 5: } \varphi(5)\\
&\text{the number of elements with order 8: } \varphi(8)\\
\\
&\text{Therefore:}\\
&\text{the number of elements with order 40: } \varphi(5) \times \varphi(8)\\
&= 4 \times 4\\
&= 16
\end{aligned}$$

v. Let $(D, \cdot)$ be a group. Given that D has exactly 10 distinct subgroups, each with 13 elements, how many elements of order 13 does D have?

We know that we have 10 distinct subgroups with 13 elements in each. Let us consider the following:

$$\begin{aligned}
&\text{Consider } H < D \ (H \text{ is a random subgroup of } D)\\
&|H| = 13\\
&\text{We want to find an element, } h \in H \text{ st } |h| = 13\\
&\forall h \in H, |h| = 13 \text{ because } |H| \text{ is prime}\\
&\text{and } |h| \text{ divides } |H|\\
\\
&\text{Therefore, we conclude that } H = < h > \text{ (Cyclic)}\\
&\text{and thus } H \text{ has } \varphi(13) \text{ elements with 13 elements}\\
&\varphi(13) = 12\\
\\
&\text{We know from a previous HW that the intersection}\\
&\text{of two subgroups that both have prime order is } \{e\}.\\
&\text{Hence } D \text{ has exactly 10 subgroups,}\\
&\text{and so it has } 10 \times 12 \text{ elements of order 13}\\
&= 120 \text{ elements}
\end{aligned}$$

Question 3:

a) Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 6 & 8 & 9 & 2 & 3 & 1 & 5 \end{pmatrix} \in S_9$. Find $|f|$.

We have an element in the symmetric group of size 9, such that $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 6 & 8 & 9 & 2 & 3 & 1 & 5 \end{pmatrix}$. In order to find the order of f, we need to consider the following:

$$f = (\ 1\ \ 4\ \ 8\ ) \circ (\ 2\ \ 7\ \ 3\ \ 6\ ) \circ (\ 5\ \ 9\ )$$

And so we know that $|f| = \mathrm{lcm}\,(3,4,2) = 12$.

$$\text{Therefore: } |f| = 12$$

b) Let $f = (\ 1\ \ 3\ \ 7\ ) \circ (\ 1\ \ 2\ \ 4\ \ 5\ ) \circ (\ 2\ \ 3\ \ 1\ \ 6\ ) \in S_7$. Find $|f|$.

Similar to part (a), we can simply proceed as follows:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

$$f = (\ 1\ \ 6\ \ 4\ \ 5\ \ 3\ \ 2\ \ 7\ )$$

Since we have now written f is the composition of disjoint cycles, we can use the result used in part (a):

$$|f| = 7$$

Question 4: Let $(D, \cdot)$ be a group st $|D| = 77$. Given that H is a normal subgroup of D st $|H| = 7$, suppose that D has exactly one subgroup with 11 elements. Prove that D is a cyclic group. Think about D/H.

Let $a \in D, a \neq e$. By Lagrange's theorem, $|a| = 7, 11 \text{ or } 77$. Let F be the unique subgroup of D with 11 elements. Choose $b \notin F \text{ and } b \notin H$. Since F is a unique subgroup with 11 elements, then $|b| \neq 11$. Therefore, $|b| = 7 \text{ or } 77$. We say that $|b| = 7$ because there is no uniqueness for the subgroup H, implying that even if $b \notin H$, it could still belong to another subgroup with 7 elements.

Let us assume that $|b| = 7$. $b \cdot H$ is an element of the group D/H ($H \lhd D$, and thus D/H is a group), and $b \cdot H \neq H$ (Because $b \notin H$). Furthermore, because $|b| = 7$, we have that $b^7 = e \in D$.

We conclude that $(b \cdot H)^7 = e \cdot H = H \in D/H$. Thus $|b \cdot H| = 7$. However, we have that $|D/H| = 11$, and by Lagrange's theorem, that means that $7|11$. This is not possible since 7 does not divide 11. This leaves us with one option, and that is $|b| = 77$.

Since we have found an element in D that has the same order as the number of elements in the group, we can conclude the following:

$$D = <b>$$

Therefore, D is a cyclic group.