Nice proof!

You may want to use fewer linebreaks.

ID: **3592**
Math A4900
Proof portfolio draft, Round 1
October 4, 2020

Statement: $D_{2n} = \langle s, r \mid s^2 = 1, r^n = 1, rs = sr^{-1}\}$. Show that if $s_1 = s$ and $s_2 = sr$, then those together with the relations

$$s_1^2 = 1, \quad s_2^2 = 1, \quad \text{and} \quad (s_1 s_2)^n = 1$$

forms and alternative presentation of D_{2n}.

Problem:	1D
No. stars:	2

Proof. We need to show that the relations and generators of the two presentations imply one another.

Lets us first show that $s_1 s_2 \in D_{2n}$ by writing s_1 and s_2 in terms of r,s and their inverses.

$s_1 = s$ and $s_1 s_2 = s^2 r = r$

Second we must show that the relations held by s_1 s_2 imply those by held in D_{2n} between r and s.

$r^n = (s_1 s_2)^n = 1$

$s^2 = s_1^2 = 1$

Note that since $s_1^2 = s_2^2 = 1$ then $s_1 = s_1^{-1}$ and $s_2 = s_2^{-1}$

Thus, rs $= (s_1\ s_2)(s_1) = s_1(s_2^{-1} s_1^{-1}) = s_1(s_1 s_2)^{-1} = sr^{-1}$.

Now let us show that r, s are in the group generated by s_1 s_2. This has already been done in the question prompt. Thus, $s_1 = s$ and $s_2 = sr$.

We must show that the relations held by r, s imply those held in the group generated by s_1 s_2.

$s_1^2 = (s)^2 = 1$

$s_2^2 = (sr)^2 = (sr)(sr) = s(rs)r = s(sr^{-1})r = s^2(r^{-1}r) = 1$

$(s_1 s_2)^n = (s(sr))^n = (s^2 r)^n = (r)^n$

We have shown that that both presentations imply one another and thus,

$$G = \langle s_1, s_2 \mid s_1^2 = s_2^2 = (s_1 s_2)^n = 1\rangle.$$

is an alternative presentation of D_{2n}.

$\square$

	Points Possible
complete	0 1 2 3 4 5
mathematically valid	0 1 2 3 4 5
readable/fluent	0 1 2 3 4 5
Total:	(out of 15)

Not sure on convention here, but you may want to use 1 proof environment instead of 2.

Problem:	2A
No. stars:	2

Statement: (1) Prove that if H and K are subgroups of a group G, then so is $H \cap K$. (2)On the other hand, prove $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.

Proof. (1) By definition all subgroups must contain the identity element. Thus, $H \cap K$ must at least be the trivial group. Thus, it is non-empty. Further, since $H \cap K$ ~~are~~ is non-empty we can apply the subgroup criterion. Since H is a subgroup then any $x, y \in H$ implies xy^{-1}. Similarly, since K is a subgroup then any $x, y \in K$ implies xy^{-1}. Hence for $x, y \in H \cap K$ we can imply that $xy^{-1} \in H \cap K$.

may want to state that $x,y \in H \cap K \Rightarrow x,y \in H,K$ and $H,K \leq G \Rightarrow xy^{-1} \in H, K$

Thus, $H \cap K$ is a subgroup. $\square$

Proof. (2) $\Rightarrow$ Assume by contradiction that $H \cup K$ is a subgroup, but $H \nsubseteq K$ and $K \nsubseteq H$. Then either H and K are disjoint or intersect for certain values.

If H and K are disjoint, then the identity element for $H \cup K$ is not unique. Hence, $H \cup K$ is not a subgroup.

Interesting approach!

an $h \in H \cup K$ s.t. $h \notin K$

$k \in K \cup H$ s.t. $k \notin H$

If they intersect on certain values, then there exists an $h \notin K$. Let us label this element h'. Similarly, there exists a $k \notin H$. Lets us label this element k'. Since $H \cup K$ is a subgroup then $H \cup K$ is closed and $hk \in H \cup K$. Consider $h'k' \in H \cup K$. Then either $h'k' \in H$ or $h'k' \in K$. Take $h'k' \in H$, since $k' \notin H$ this is a contradiction. Take $h'k' \in K$, since $h' \notin K$ this is a contradiction.

Thus, if $H \cup K$ is a subgroup, then $H \subseteq K$ or $K \subseteq H$.

$\Leftarrow$ Assume $H \subseteq K$, then $H \cup K = K$. Assume further that $K \subseteq H$, then $H \cup K = H$. Since for each respective case $H \cup K = K$ or $H \cup K = H$, and H and K are subgroups, then $H \cup K$ is a subgroup.

$\square$

Nice job!

1

	Points Possible					
complete	0	1	2	3	4	5
mathematically valid	0	1	2	3	4	5
readable/fluent	0	1	2	3	4	5
Total:					(out of 15)	

Statement: Let G act on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \quad \text{when} \quad a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation.

Problem:	3B
No. stars:	1

Proof. Assume $a \sim b$ defined by $a = g \cdot b$. We want to show that $a \sim b$ is reflexive, symmetric and transitive.

Reflexive: $a = 1 \cdot a =$ a, since $1 \in G$. Thus, $a \sim b$ is symmetric. Since $a \sim a$

Nice approach!

Symmetric: We want to show that $a = g \cdot b$ implies $b = g \cdot a$. ← use $b = g^{-1} \cdot a$ since the 2 gs are not necessarily equal

Notice that $a = g \cdot b$ implies $ab^{-1} = g$. Since $ab^{-1} = g$, then $(ab^{-1})^{-1} \in G$ and thus $ba^{-1} \in G$. Consequently, then $ba^{-1} = g$, which further implies $b = g \cdot a$. Thus, $a \sim b$ is symmetric.

Transitive : We want to show that if $a = g \cdot b$ and $b = g \cdot c$, then $a = g \cdot c$. ←

Notice that $a = g \cdot b$ implies $ab^{-1} = g$ and $b = g \cdot c$ implies $bc^{-1} = g$. Let us multiply $ab^{-1}bc^{-1}$. Since $ab^{-1}bc^{-1} \in G$, then $ab^{-1}bc^{-1} = g$. Take note that $g = ab^{-1}bc^{-1} = a(b^{-1}b)c^{-1} = ac^{-1}$. Finally, we have that $g = ac^{-1}$ which further implies that $g \cdot c = a$. Thus, $a \sim b$ is transitive.

$ab^{-1}bc^{-1} = g \cdot g = g^2$

Because $a \sim b$ is reflexive, symmetric and transitive $a \sim b$ is an equivalence relation. □

	Points Possible
complete	0 1 2 3 4 5
mathematically valid	0 1 2 3 4 5
readable/fluent	0 1 2 3 4 5
Total:	(out of 15)

Statement: Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Problem:	1E
No. stars:	3

Proof. Assume that an element τ in S_n can be written as the product of disjoint cycles, that is, suppose $\tau = \sigma_1\sigma_2 \ldots\sigma_n$. define i as well

Make sure to define m before this

With this assumption we can write, $\tau^i = (\sigma_1\sigma_2\ldots\sigma_n)^i = 1$, where $1 \leqslant n < m-1$. Because these disjoint cycles are commutative we have $\tau^i = \sigma_1^i\sigma_2^i\ldots\sigma_n^i = 1$. This implies further that that $\sigma_1^i = \sigma_2^i = \ldots = \sigma_n^i = 1$. Which further implies the orders of the cycles are equal, and less than m, ~~Where~~ where m is the order of S_n. Let us denote the cycle orders as m_n for all n. Thus we have that $m_1 + m_2 + \ldots + m_n = m$. This implies that there exists and integer p such that $p \times m_n = m$. Therefore m is the least common multiple of the cycle lengths $m_1, m_2, \ldots m_n$. $\square$

Why is this sum true?

Is $p \times m_n$ necessarily the lcm of $m_1, m_2, \ldots, m_n$?

Really nice job overall on these proofs!

	Points Possible
complete	0 1 2 3 4 5
mathematically valid	0 1 2 3 4 5
readable/fluent	0 1 2 3 4 5
Total:	(out of 15)