Problem 1. Let M be a fixed 2×2 real matrix with determinant 1. Define $\rho : SL(2,\mathbb{R}) \to SL(2,\mathbb{R})$ according to $\rho(A) = MAM^{-1}$. Show that ρ is an isomorphism.S

Solution:

M and A have a determinant of one because $M, A \in SL(2,\mathbb{R})$. M^{-1} also has a determinant of 1 because of the property, $\det(ab) = \det(a) \cdot \det(b)$ where a, b are matricies. So, $\det(MM^{-1}) = \det(I) = 1 = \det(M) \cdot \det(M^{-1})$. Since all of these have a determinant of one, $\det(MAM^{-1}) = \det(MA) \cdot \det(M^{-1}) = \det(M)\det(A)\det(M^{-1}) = 1$. This shows that the product is always in $SL(2,\mathbb{R})$ and ρ is well defined.

ρ is also one-to-one. Assume $\rho(A_1) = \rho(A_2),\ A_1, A_2 \in \mathrm{SL}(2,\mathbb{R})$. I want to show that this implies $A_1 = A_2$. I rewrite $\rho(A_1) = \rho(A_2)$ as $MA_1M^{-1} = MA_2M^{-1}$. By left multiplying both sides by M^{-1} and then right multiplying by M I get, $A_1 = A_2$. So,

$$\rho(A_1) = \rho(A_2) \implies A_1 = A_2.$$

This shows that ρ is one-to-one.

ρ is onto because $\forall y \in SL(2,\mathbb{R}), \exists x \in SL(2,\mathbb{R})\ s.t\ \rho(x) = y$.

To show ρ is operation preserving, I will show that $\rho(A_1A_2) = \rho(A_1)\rho(A_2)$. Rewriting the left hand side I get $\rho(A_1A_2) = MA_1A_2M^{-1}$. Rewriting the right hand side I get

$$\rho(A_1)\rho(A_2) = MA_1M^{-1}MA_2M^{-1} = MA_1IA_2M^{-1} = MA_1A_2M^{-1}.$$

Since

$$\rho(A_1A_2) = MA_1M^{-1} = \rho(A_1)\rho(A_2),$$

this shows that ρ is operation preserving.

Since ρ is well defined, forms a bijection between $SL(2,\mathbb{R})$ and is operation preserving, ρ is an isomorphism.

Problem 2. Prove that if G is a cyclic group of order n, then $G \cong \mathbb{Z}_n$.

Solution:

Since G is a cyclic group, $G = \langle a \rangle$ where $a^n = e,\ a \in G,\ n \in \mathbb{Z}$. To show G is isomorphic to $\mathbb{Z}_n$, I define the function $\phi : G \to \langle \mathbb{Z}_n, + \rangle$ as $\phi(a^k) = k,\ 0 \leq k \leq n$. This function is well defined because G has order n and so does $\mathbb{Z}_n$. Since this is true, when k is between 0 and n it follows that the domain will always map to the codomain because $\mathbb{Z}_n$ is all values y where $0 \leq y \leq n$.

To show that ϕ is one-to-one, assume $\phi(a^{k_1}) = \phi(a^{k_2})$. I want to show that this implies $k_1 = k_2$. Rewriting using the definition of ϕ, I get $\phi(a^{k_1}) = \phi(a^{k_2}) = k_1 = k_2$. This shows that ϕ is one-to-one.

ϕ is also onto because for every element in $\mathbb{Z}_n$, there is a k in G such that $\phi(a^k) \in \mathbb{Z}_n$. That k is $k = y$.

I want to show that ϕ is operation preserving. That is that, $\phi(a^{k_1}a^{k_2}) = \phi(a^{k_1}) + \phi(a^{k_2})$. Rewriting the left hand side I get $\phi(a^{k_1+k_2}) = k_1 + k_2$. Rewriting the right hand side I get $\phi(a^{k_1}) + \phi(a^{k_2}) = k_1 + k_2$. Since $\phi(a^{k_1}a^{k_2}) = k_1 + k_2 = \phi(a^{k_1}) + \phi(a^{k_2})$, this shows that ϕ is operation preserving.

Since ϕ is well defined, forms a bijection between G and $\mathbb{Z}_n$ and is operation preserving, ϕ forms a group isomorphism between G and $\mathbb{Z}_n$. Therefore, $G \cong \mathbb{Z}_n$.

Problem 3. Let $\langle G, * \rangle$ and $\langle H, \circ \rangle$ be finite cyclic groups such that $|G| = |H|$. Prove that $G \cong H$.

Proof.

Since $\langle G, * \rangle$ and $\langle H, \circ \rangle$ are two finite cyclic groups, they can be expressed in terms of their generators. That is, $\langle G, * \rangle = \langle a \rangle,\ a \in G$ and $\langle H, \circ \rangle = \langle b \rangle,\ b \in H$. This means that $\forall k \in \mathbb{Z}_n,\ a^k \in G$ where $|G| = n$ and since $|G| = |H|$, $b^k \in H$. So, it is easy to see that $G = \{a^0, a^1, ..., a^{n-1}\}$ and $H = \{b^0, b^1, ..., b^{n-1}\}$. Seeing it this way makes it clear that there is a function $\phi : \langle G, * \rangle \to \langle H, \circ \rangle$. That is,

$$\phi(a^k) = b^k.$$

To show that ϕ is one-to-one I will show that $\phi(a^k) = \phi(a^r)$ implies $a^k = a^r$. Rewriting $\phi(a^k) = \phi(a^r)$, I get $b^k = b^r$. Since $b^k = b^r$ implies $k = r$, this shows that $a^k = a^r$.

It is clear to see that for every $b^k \in H$ there is an $a^k \in G$ such that $\phi(a^k) = b^k$ because $\phi(a^k) = b^k$ is the definition of the function.

I want to show that ϕ is operation preserving. To do this I will show that $\phi(a^k * a^r) = \phi(a^k) \circ \phi(a^r)$. By rewriting the left hand side of this equation I get $\phi(a^k * a^r) = \phi(a^{k+r}) = b^{k+r}$. Rewriting the right hand side I get $\phi(a^k) \circ \phi(a^r) = b^k \circ b^r = b^{k+r}$. Since $\phi(a^k * a^r) = b^{k+r} = \phi(a^k) \circ \phi(a^r)$, this shows that ϕ is operation preserving.

Since ϕ is well defined, forms a bijection between $\langle G, * \rangle$ and $\langle H, \circ \rangle$, and is operation preserving, ϕ is an isomorphism between $\langle G, * \rangle$ and $\langle H, \circ \rangle$. Since this isomorphism exists, $\langle G, * \rangle \cong \langle H, \circ \rangle$ when $|G| = |H|$. $\square$

Problem 4. Let G be a group. Show that the function $f : G \to G$ defined by

$$f(a) = a^{-1}$$

is an isomorphism (hence an automorphism) iff G is abelian.

Solution:

f is well defined because the inverse exists for every element in G because G is a group. To show that f is one-to-one, I will show that $f(a_1) = f(a_2) \implies a_1 = a_2$. I will rewrite the RHS of the implication using the definition of f as $f(a_1) = f(a_2) = a_1^{-1} = a_2^{-1}$. Since it is a property that inverses are unique in groups, it follows that, $a_1 = a_2$. This shows that f is one-to-one.

f is onto because it is a property of groups that for every element in G, there is an inverse. So, the inverse of $a^{-1} = (a^{-1})^{-1} = a$. So $\forall y \in G, \exists x \in G\ s.t\ f(x) = y$. This shows that f is onto.

I want to show that f is operation preserving. To do this I can show that $f(a_1 a_2) = f(a_1) f(a_2)$. I can rewrite the RHS as $f(a_1 a_2) = (a_1 a_2)^{-1}$. Then I rewrite the LHS as $f(a_1) f(a_2) = a_1^{-1} a_2^{-1}$. I can multiply $a_1 a_2$ on both sides of $(a_1 a_2)^{-1} = a_1^{-1} a_2^{-1}$ to get $e = a_1 a_2 a_1^{-1} a_2^{-1}$ where e is the identity element in G. Here, if G is not abelian then I cannot show that f is operation preserving. But if G is abelian, I can rewrite the equation to be $e = a_1 a_2 a_1^{-1} a_2^{-1} = a_1 a_1^{-1} a_2 a_2^{-1} = e$. This shows that f is operation preserving iff G is abelian.

Since f is a well defined function, forms a bijection from G to iteself, and is operation preserving iff G is abelian, there is an isomorphism that exists on G iff G is abelian.

Problem 5. Let a be a fixed element of a group G. The automorphism $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ is called the **inner automorphism induced by** a.

(a) Show that $\phi_a\phi_b = \phi_{ab}$ for any $a, b \in G$

(b) Show that $(\phi_a)^{-1} = \phi_{a^{-1}}$ for any $a \in G$

(c) Prove that the set of all inner automorphisms, denoted $\text{Inn}(G)$, is a group under function composition.

Solution:

(a) I need to show that $\phi_a\phi_b = \phi_{ab}$. That is, $\phi_a(\phi_b) = \phi_{ab}$. By rewriting the RHS, I get $\phi_a(bxb^{-1}) = abxb^{-1}a^{-1}$. Rewriting the LHS, I get $\phi_{ab} = abx(ab)^{-1}$. Setting the rewritten RHS equal to the rewritten LHS I get $abxb^{-1}a^{-1} = abx(ab)^{-1}$. Right multiplying both sides of the equation by ab I get $abxb^{-1}a^{-1}ab = abx(ab)^{-1}ab$. Rewriting, I get $abxee = abxee$ where e is the identity element in G. This shows that $\phi_a\phi_b = \phi_{ab}$.

(b) I need to show that $(\phi_a)^{-1} = \phi_{a^{-1}}$. To do this I will rewrite the RHS as $(\phi_a)^{-1} = (axa^{-1})^{-1}$ and the LHS as $\phi_{a^{-1}} = a^{-1}xa$. Setting these equations equal to eachother I get $(axa^{-1})^{-1} = a^{-1}xa$. Since these are all elements of G because of the closure of the binary operation, all of the products inverses exist. So, taking the inverse of both sides of the equation I get $axa^{-1} = (a^{-1}xa)^{-1}$. It follows that $(axa^{-1})^{-1} = ((a^{-1}xa)^{-1})^{-1} = a^{-1}xa$. Since $(\phi_a)^{-1} = ((a^{-1}xa)^{-1})^{-1} = a^{-1}xa = \phi_{a^{-1}}$, this shows that $(\phi_a)^{-1} = \phi_{a^{-1}}$.

(c) *Proof.*

$\text{Inn}(G)$ is closed under $\circ$ because for any $a, b \in G$, $\phi_a \circ \phi_b = \phi_{ab},\ \phi_{ab} \in \text{Inn}(G)$. This is shown in part (a). Therefore $\text{Inn}(G)$ is closed under $\circ$.
To find the identity, I want to find an element $\phi_{\bar{e}}$ such that $\phi_f \circ \phi_{\bar{e}} = \phi_f$. That is, where $f\bar{e}x\bar{e}^{-1}f^{-1} = fxf^{-1}$. This is when $\bar{e} = e$ where $e \in G$. So, the identity is ϕ_e.
In part (b) I have shown that for any $a \in G,\ (\phi_a)^{-1} = \phi_{a^{-1}}$. So the inverse exists and is $\phi_{a^{-1}}$
To show that $\langle \text{Inn}(G), \circ \rangle$ has the associative property, I will show that $\phi_a \circ (\phi_b \circ \phi_c) = (\phi_a \circ \phi_b) \circ \phi_c$. From part (a) I know that $\phi_a \circ \phi_b = \phi_{ab}$. So, rewriting the RHS of $\phi_a \circ (\phi_b \circ \phi_c) = (\phi_a \circ \phi_b) \circ \phi_c$, I get $\phi_a \circ (\phi_{bc}) = \phi_{a(bc)} = \phi_{abc}$ because of the associative property which is in G. Rewriting the LHS I get, $(\phi_a \circ \phi_b) \circ \phi_c = \phi_{ab} \circ \phi_c = \phi_{abc}$. Since, $\phi_a \circ (\phi_b \circ \phi_c) = \phi_{abc} = (\phi_a \circ \phi_b) \circ \phi_c$, $\langle \text{Inn}(G), \circ \rangle$ has the associative property.
Since $\langle \text{Inn}(G), \circ \rangle$ has an identity, an inverse for all elements in it, associativity and is closed under $\circ$, $\langle \text{Inn}(G), \circ \rangle$ is a group. □

Problem 6. Find the order of $\big((1,2,5)(1,3,4), 5, \omega^{15}\big)$ in the direct product $S_6 \oplus \mathbb{Z}_8 \oplus U_{18}$, where $\omega = \text{cis}(\frac{2\pi}{18})$

Solution:

Using theorem 8.2.1, $\text{ord}((1,2,5)(1,3,4), 5, \omega^{15})) = \text{LCM}(\text{ord}_{S_6}((1,2,5)(1,3,4)), \text{ord}_{\mathbb{Z}_8}(5), \text{ord}_{U_{18}}(\omega^{15}))$.
(1,2,5)(1,3,4) $= \left(\begin{smallmatrix}1&2&3&4&5&6\\2&5&3&4&1&6\end{smallmatrix}\right) \circ \left(\begin{smallmatrix}1&2&3&4&5&6\\3&2&4&1&5&6\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2&3&4&5&6\\3&5&4&2&1&6\end{smallmatrix}\right) = (1,3,4,2,5)$. The order of (1,2,5)(1,3,4) = (1,3,4,2,5) is 5 because the order of a k-cycle is k.
For $5 \in \mathbb{Z}_8,\ \langle 5 \rangle = \{5, 2, 7, 4, 1, 6, 3, 0\}$. So $\text{ord}_{\mathbb{Z}_8}(5) = 8$.
Since $U_{18} \cong \mathbb{Z}_{18},\ \text{ord}_{\mathbb{Z}_{18}}(15) = \text{ord}_{U_{18}}(\omega^{15})$. For $15 \in \mathbb{Z}_{18},\ \langle 15 \rangle = \{15, 12, 9, 6, 3, 0\}$. Therefore $\text{ord}_{\mathbb{Z}_{18}}(15) = 6$.
Using theorem 8.2.1, $\text{ord}((1,2,5)(1,3,4), 5, \omega^{15})) = \text{LCM}(\text{ord}_{S_6}((1,2,5)(1,3,4)), \text{ord}_{\mathbb{Z}_8}(5), \text{ord}_{U_{18}}(\omega^{15})) = \text{LCM}(8, 5, 6) = 120$.

Problem 7. Find four non-isomorphic groups of order 50.

Solution:

$\mathbb{Z}_{50}$ has order 50 because its generator is 1. D_n has order $2n$, so D_{25} has order 50 and is not isomorphic to $\mathbb{Z}_{50}$ because it is not abelian. I used theorem 8.1.1 to figure out that $|\mathbb{Z}_{10} \oplus \mathbb{Z}_5| = |\mathbb{Z}_{10}| \cdot |\mathbb{Z}_5| = 50$. $\mathbb{Z}_{10} \oplus \mathbb{Z}_5 \ncong \mathbb{Z}_{50}$ because it is not cyclic. This is because if $\mathbb{Z}_{10} \oplus \mathbb{Z}_5$ was cyclic then $\mathbb{Z}_{10} \oplus \mathbb{Z}_5 = \langle (a,b) \rangle$ where $\mathbb{Z}_{10} = \langle a \rangle$ and $\mathbb{Z}_5 = \langle b \rangle$, but $\text{ord}_{\mathbb{Z}_{10} \oplus \mathbb{Z}_5}((a,b)) = LCM(10,5) = 10$. This is a contradiction because the order of $\mathbb{Z}_{10} \oplus \mathbb{Z}_5$ is 50. Therefore, $\mathbb{Z}_{10} \oplus \mathbb{Z}_5$ is not cyclic. Also, $\mathbb{Z}_{10} \oplus \mathbb{Z}_5 \ncong D_{25}$ because D_{25} is not abelian but $\mathbb{Z}_{10} \oplus \mathbb{Z}_5$ is abelian by the fundamental theorem of finite abelian groups. That is, because $\mathbb{Z}_{10} \oplus \mathbb{Z}_5 = \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5$. Which can better be seen as $\mathbb{Z}_{5^2} \oplus \mathbb{Z}_2$. Finally, $\mathbb{Z}_5 \oplus D_5$ is the last group. This is not isomorphic to $\mathbb{Z}_{50}$ because it is not abelian and $\mathbb{Z}_{50}$ is. This is also not isomorphic to $\mathbb{Z}_{10} \oplus \mathbb{Z}_5$ because $\mathbb{Z}_{10} \ncong \mathbb{Z}_5$ or D_5. Finally, this is not isomorphic to D_{25}. So the groups are, $\mathbb{Z}_{50}, D_{25}, \mathbb{Z}_{10} \oplus \mathbb{Z}_5$, and $\mathbb{Z}_5 \oplus D_5$.

Problem 8. Prove or disprove: $\mathbb{Z}_4 \oplus \mathbb{Z}_{15} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$?

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{15} \ncong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}.$$

Proof.
It is clear that $|\mathbb{Z}_4 \oplus \mathbb{Z}_{15}| = 4 \cdot 15 = 60 = 10 \cdot 6 = |\mathbb{Z}_6 \oplus \mathbb{Z}_{10}|$. If $\mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ is cyclic, then $\mathbb{Z}_4 \oplus \mathbb{Z}_{15} = \langle (a,b) \rangle$ where $\mathbb{Z}_4 = \langle a \rangle, \mathbb{Z}_{15} = \langle b \rangle$. $\text{ord}_{\mathbb{Z}_4 \oplus \mathbb{Z}_{15}}((a,b)) = \text{LCM}(\text{ord}_{\mathbb{Z}_4}(a), \text{ord}_{\mathbb{Z}_{15}}(b)) = \text{LCM}(4,15) = 60 = |\mathbb{Z}_4 \oplus \mathbb{Z}_{15}|$. Therefore $\mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ is cyclic.

If $\mathbb{Z}_6 \oplus \mathbb{Z}_{10}$ is cyclic, then $\mathbb{Z}_6 \oplus \mathbb{Z}_{10} = \langle (a,b) \rangle$ where $\mathbb{Z}_6 = \langle a \rangle$, $\mathbb{Z}_{10} = \langle b \rangle$. But, $\text{ord}_{\mathbb{Z}_6 \oplus \mathbb{Z}_{10}}((a,b)) = \text{LCM}(\text{ord}_{\mathbb{Z}_6}(a), \text{ord}_{\mathbb{Z}_{10}}) = \text{LCM}(6,10) = 30 \neq 60 = |\mathbb{Z}_6 \oplus \mathbb{Z}_{10}|$. Therefore $\mathbb{Z}_6 \oplus \mathbb{Z}_{10}$ is not cyclic.

Since $\mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ is cyclic and $\mathbb{Z}_6 \oplus \mathbb{Z}_{10}$ is not cyclic, by theorem 7.4.2, $\mathbb{Z}_4 \oplus \mathbb{Z}_{15} \ncong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$. □

Problem 9. Knowing that $S_3 \oplus \mathbb{Z}_2$ has 12 elements, it may be isomorphic to $\mathbb{Z}_{12}, \mathbb{Z}_6 \oplus \mathbb{Z}_2, A_4$, or D_6. Which one? Why?

Solution:

To find the elements with order 2 in $S_3 \oplus \mathbb{Z}_2$, I need to find the pairs (a,b) such that $(a,b)^2 = e$. Using theorem 8.2.1, I find that $\text{ord}_{S_3 \oplus \mathbb{Z}_2}((a,b)) = \text{LCM}(\text{ord}_{S_3}(a), \text{ord}_{\mathbb{Z}_2}(b))$ but I want to find where the order is 2, so that is when $\text{LCM}(\text{ord}_{S_3}(a), \text{ord}_{\mathbb{Z}_2}(b)) = 2 = \text{LCM}(2,1), \text{LCM}(1,2)$, and $\text{LCM}(2,2)$. By inspection of S_3 and $\mathbb{Z}_2$, it follows that there are 3 elements that satisfy $\text{ord}_{S_3}(a) = 2$ and $\text{ord}_{\mathbb{Z}_2}(b) = 1$. There is also only one element that satisfies $\text{ord}_{S_3}(a) = 1$ and $\text{ord}_{\mathbb{Z}_2}(b) = 2$. Another 3 elements satisfies when $\text{ord}_{S_3}(a) = 2$ and $\text{ord}_{\mathbb{Z}_2}(b) = 2$. So, in total, there are 7 elements in $S_3 \oplus \mathbb{Z}_2$. Doing the same process for $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ I find that there is one element in $\mathbb{Z}_6$ with order 2 which is a^k when $\frac{6}{\gcd(6,k)} = 2$. So, $k = 3$ is the only solution which means $\text{ord}(\langle 1^3 \rangle) = 2 = \text{ord}(\langle 3 \rangle) = 2$. Since there is one element of order 2, again by theorem 8.2.1, I find that there are only 3 elements of order 2 in $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ therefore $S_3 \oplus \mathbb{Z}_2 \ncong \mathbb{Z}_6 \oplus \mathbb{Z}_2$. Doing a similar process for $\mathbb{Z}_{12}$, I find that there is one element in $\mathbb{Z}_{12}$ of order 2, that is when $|a^k| = \frac{12}{\gcd(12,k)} = 2$. This is when $k = 6$, so $|\langle 1^6 \rangle| = |\langle 6 \rangle| = 2$. So, since there is only one element of order 2 in $\mathbb{Z}_{12}$, but 7 in $S_3 \oplus \mathbb{Z}_2$, $S_3 \oplus \mathbb{Z}_2 \ncong \mathbb{Z}_{12}$. A similar process is done for A_4. I find that there are only 6 elements of order 2. This is because all transpositions of S_4 are of order 2 and in A_4. So, since there are only 6 elements of order 2 in A_4 and 7 elements of order 2 in $S_3 \oplus \mathbb{Z}_2$, $S_3 \oplus \mathbb{Z}_2 \ncong A_4$. Since all other groups have been ruled out, $S_3 \oplus \mathbb{Z}_2 \cong D_6$.

Problem 10. Consider $\text{Aut}(\mathbb{Z}_{15})$.

(a) Tabulate the images of each automorphism over $\mathbb{Z}_{15}$

(b) It is known that $\text{Aut}(\mathbb{Z}_{15})$ is abelian. Based on the number of automorphisms you have found, what do you think $\text{Aut}(\mathbb{Z}_{15})$ could possibly be isomorphic to (as a direct product)? Can you determine which one it is isomorphic to?

Solution:

(a) $\text{Aut}(\mathbb{Z}_{15}) = \{f_1, f_2, f_4, f_7, f_8, f_{11}, f_{13}, f_{14}\}$.

i	$f_i(0)$	$f_i(1)$	$f_i(2)$	$f_i(3)$	$f_i(4)$	$f_i(5)$	$f_i(6)$	$f_i(7)$	$f_i(8)$	$f_i(9)$	$f_i(10)$	$f_i(11)$	$f_i(12)$	$f_i(13)$	$f_i(14)$
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
4	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
7	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	0	8	1	9	2	10	3	11	4	12	5	13	6	14	7
11	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
13	0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

(b) Using theorem 7.5.2, $\text{Aut}(\mathbb{Z}_{15}) \cong U(15)$ and $U(15) \cong U(5) \oplus U(3)$ by corollary 8.3.2, so by transitivity of isomorphisms, $\text{Aut}(\mathbb{Z}_{15}) \cong U(5) \oplus U(3)$.

Problem 11. Let $\mathcal{R} = \langle R_{\frac{360^\circ}{n}} \rangle$ be the subgroup of rotations in D_n. Prove or disprove: $D_n \cong \mathcal{R} \oplus \mathbb{Z}_2$

$$D_n \ncong \mathcal{R} \oplus \mathbb{Z}_2.$$

Proof.

It is known that $\langle R_{\frac{360^\circ}{n}} \rangle \cong \mathbb{Z}_n$. If $D_n \cong \mathcal{R} \oplus \mathbb{Z}_2$, then the amount of elements of order 2 in D_n and $\mathcal{R} \oplus \mathbb{Z}_2$ are the same. Suppose $D_n \cong \mathcal{R} \oplus \mathbb{Z}_2$, then $D_n \cong \mathbb{Z}_n \oplus \mathbb{Z}_2$. Let $n = 6$. It follows that $D_6 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2$. But from problem 9, I have found that $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ has only 3 elements and that have order 2 and D_6 has 7 elements of order 2. This forms a contradiction with the fact that if $D_n \cong \mathcal{R} \oplus \mathbb{Z}_2$, then the amount of elements of order 2 in D_n and $\mathcal{R} \oplus \mathbb{Z}_2$ are the same. Therefore $D_n \ncong \mathcal{R} \oplus \mathbb{Z}_2$ in general. □