MATH 417, HOMEWORK 4

CHARLES ANCEL

Exercise 1. Determine whether there is an isomorphism between $\Phi(5)$ and $\Phi(8)$.

SOLUTION

To determine whether there is an isomorphism between $\Phi(5)$ and $\Phi(8)$, we will investigate the structures of the groups $\Phi(5)$ and $\Phi(8)$.

Structure of $\Phi(5)$. The group $\Phi(5)$ represents the group of units modulo 5, i.e., the integers less than 5 that are coprime to 5. The elements of $\Phi(5)$ are:

$$\Phi(5) = \{1, 2, 3, 4\}.$$

The group operation is multiplication modulo 5. We will compute the multiplication table for $\Phi(5)$:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Structure of $\Phi(8)$. The group $\Phi(8)$ represents the group of units modulo 8. The elements of $\Phi(8)$ are:

$$\Phi(8) = \{1, 3, 5, 7\}.$$

The group operation is multiplication modulo 8. We will compute the multiplication table for $\Phi(8)$:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Order and Group Structure. To determine if $\Phi(5)$ and $\Phi(8)$ are isomorphic, we compare their structures:

- Both groups have the same order, $|\Phi(5)| = |\Phi(8)| = 4$.

- Both groups are abelian (commutative) and have the same number of elements.

1

– We need to compare the orders of their elements and their multiplication tables to determine if they are structurally identical.

Comparison of Elements. In $\Phi(5)$:

– 1 has order 1.

– 2 and 3 have order 4.

– 4 has order 2.

In $\Phi(8)$:

– 1 has order 1.

– 3 and 5 have order 4.

– 7 has order 2.

The orders of elements are the same in both groups, indicating they have the same group structure.

Existence of an Isomorphism. Since both groups $\Phi(5)$ and $\Phi(8)$ have the same order and the same order of elements, and their multiplication tables exhibit the same structure, they are isomorphic. An isomorphism can be constructed by mapping corresponding elements of the same order. For instance:

$$
\begin{array}{ccc}
\Phi(5) & \to & \Phi(8) \\
1 & \mapsto & 1 \\
2 & \mapsto & 3 \\
3 & \mapsto & 5 \\
4 & \mapsto & 7
\end{array}
$$

This mapping preserves the group operation, and thus $\Phi(5)$ and $\Phi(8)$ are isomorphic.

Conclusion. The groups $\Phi(5)$ and $\Phi(8)$ are isomorphic. The isomorphism can be established by mapping elements with the same orders and ensuring the preservation of the group operation.

Exercise 2. Let $(M, \cdot)$ be a monoid. Say that a subset $N \subseteq M$ is a submonoid if (1) the product $a, b \mapsto ab$ on M restricts to a function $N \times N \to N$ and (2) N with the restricted operation is a monoid.

    a. Show that a subset N of a monoid M is a submonoid if and only if

      (i) if $a, b \in N$, then $ab \in N$;

      (ii) there exists an element $e' \in N$ such that $e'a = a = ae' \; \forall \, a \in N$.

    b. Let $M := \mathrm{Mat}_{2 \times 2}(\mathbb{R})$ be the monoid of 2×2 real matrices, with operations given by matrix multiplication. Let N be the subset of M consisting of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$. Show that N is a submonoid of M.

    c. Show that if N is a submonoid of M, then the identity element of N might not be the same as the identity element of M. (This is different from the case of subgroups, where we could show that the identity element of the subgroup must be equal to the identity element of the larger group.)

Solution

a. Necessary and Sufficient Conditions for Submonoids.

Proof.

    To show that a subset N of a monoid M is a submonoid if and only if:

    (i) $\forall \, a, b \in N$, $ab \in N$;

    (ii) There exists an element $e' \in N$ such that $e'a = a = ae' \; \forall \, a \in N$.

Sufficiency. Assume that conditions (i) and (ii) hold.

    – **Closure**: Condition (i) ensures that N is closed under the operation $\cdot$, meaning the product of any two elements in N is still in N.

    – **Identity**: Condition (ii) ensures that N contains an identity element e' for the operation restricted to N.

    – **Associativity**: The operation $\cdot$ is associative on M by definition of a monoid, and hence remains associative on the subset N.

    Thus, N with the restricted operation $\cdot$ forms a monoid, making it a submonoid of M.

Necessity. Assume N is a submonoid of M.

    – By definition, if N is a submonoid, the product $a \cdot b$ of any two elements $a, b \in N$ must also be in N, satisfying condition (i).

    – Since N is a monoid, it must contain an identity element e' such that $e'a = a = ae'$ for all $a \in N$, satisfying condition (ii).

Thus, the conditions (i) and (ii) are necessary for N to be a submonoid.

$\square$

b. N is a Submonoid of $M := \mathbf{Mat}_{2 \times 2}(\mathbb{R})$.

Proof.

Let M be the monoid of 2×2 real matrices under matrix multiplication, and let N be the subset of M consisting of matrices of the form:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

Closure. Consider two matrices in N:

$$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}.$$

Their product is:

$$A \cdot B = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}.$$

Since $ab \in \mathbb{R}$, the resulting matrix is still of the form $\begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix}$ and hence belongs to N. Therefore, N is closed under matrix multiplication.

Identity Element. The identity element in M is the 2×2 identity matrix:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

However, this does not belong to N. The identity element within N is:

$$E' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

which satisfies:

$$E'A = A = AE' \quad \forall\, A \in N.$$

Since N contains this element E' that acts as an identity for all its elements, and N is closed under matrix multiplication, N is a submonoid of M.

$\square$

c. Identity Element in a Submonoid.

Proof.

Let N be a submonoid of a monoid M. We need to show that the identity element of N might not be the same as the identity element of M.

Example. Consider $M := \mathrm{Mat}_{2\times 2}(\mathbb{R})$ with the identity element:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let N be the submonoid of matrices of the form:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

We have shown in part (b) that the identity element of N is:

$$E' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

which is different from the identity element of M.

Conclusion. This example demonstrates that the identity element of a submonoid N can be different from the identity element of the larger monoid M.

$\square$

Exercise 2.2.4. Let $H \subseteq S_4$ be the subset consisting of: all 3-cycles, all products of disjoint 2-cycles, and the identity.

    a. Show that $U := \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is a subgroup of S_4.

    b. Show that the product of any two 3-cycles in S_4 is either: the identity, a 3-cycle, or a product of two disjoint 2-cycles.

    c. Show that the product of a 3-cycle in S_4 with any product of two disjoint 2-cycles is a 3-cycle.

    d. Show that H is a subgroup of S_4.

SOLUTION

a. U is a Subgroup of S_4.

Proof.

    Let $U = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

    To show that U is a subgroup of S_4, we will verify the subgroup criteria:

    – **Closure**: Check that the product of any two elements in U is still in U.

    – **Identity**: Verify that the identity element e is in U.

    – **Inverses**: Verify that the inverse of any element in U is also in U.

Closure. We compute the products of the elements in U:

$$(1\ 2)(3\ 4) \cdot (1\ 2)(3\ 4) = e,$$
$$(1\ 2)(3\ 4) \cdot (1\ 3)(2\ 4) = (1\ 4)(2\ 3),$$
$$(1\ 2)(3\ 4) \cdot (1\ 4)(2\ 3) = (1\ 3)(2\ 4),$$
$$(1\ 3)(2\ 4) \cdot (1\ 3)(2\ 4) = e,$$
$$(1\ 3)(2\ 4) \cdot (1\ 4)(2\ 3) = (1\ 2)(3\ 4),$$
$$(1\ 4)(2\ 3) \cdot (1\ 4)(2\ 3) = e.$$

    Since all products are in U, U is closed under the group operation.

Identity. The identity element e is in U by definition.

Inverses. We find the inverses of the elements in U:

$$e^{-1} = e,$$
$$((1\ 2)(3\ 4))^{-1} = (1\ 2)(3\ 4),$$
$$((1\ 3)(2\ 4))^{-1} = (1\ 3)(2\ 4),$$
$$((1\ 4)(2\ 3))^{-1} = (1\ 4)(2\ 3).$$

    Since all inverses are in U, every element has an inverse in U.

Conclusion. Thus, U is a subgroup of S_4.

<div align="right">□</div>

b. Product of Two 3-Cycles in S_4.

Proof.

Let σ and τ be 3-cycles in S_4. We need to show that $\sigma\tau$ is either the identity, a 3-cycle, or a product of two disjoint 2-cycles.

Case 1: σ and τ are Disjoint. Suppose $\sigma = (a\ b\ c)$ and $\tau = (d\ e\ f)$, where $\{a, b, c\} \cap \{d, e, f\} = \emptyset$.

In this case, $\sigma\tau = \tau\sigma = \sigma \circ \tau$ as they act on disjoint sets. Thus, $\sigma\tau$ is a product of two disjoint 3-cycles, but because there are no such elements in S_4, it reduces to a product of disjoint 2-cycles, i.e., e.

Case 2: σ and τ Share Two Elements. Suppose $\sigma = (a\ b\ c)$ and $\tau = (a\ c\ b)$.

$$\sigma\tau = (a\ b\ c)(a\ c\ b) = e.$$

In this case, $\sigma\tau$ is the identity.

Case 3: σ and τ Share One Element. Suppose $\sigma = (a\ b\ c)$ and $\tau = (a\ c\ d)$.

$$\sigma\tau = (a\ b\ c)(a\ c\ d) = (a\ b\ d).$$

In this case, $\sigma\tau$ is a 3-cycle.

Conclusion. The product of any two 3-cycles in S_4 is either the identity, a 3-cycle, or a product of two disjoint 2-cycles.

<div align="right">□</div>

c. Product of a 3-Cycle and a Product of Two Disjoint 2-Cycles.

Proof.

Let $\sigma = (a\ b\ c)$ be a 3-cycle and $\tau = (d\ e)(f\ g)$ be a product of two disjoint 2-cycles in S_4.

Case 1: σ and τ are Disjoint. Suppose $\{a, b, c\} \cap \{d, e, f, g\} = \emptyset$.

In this case, $\sigma\tau = \tau\sigma = \sigma \circ \tau$. Since τ does not affect the elements of σ, $\sigma\tau$ is just a permutation of σ, remaining a 3-cycle.

Case 2: σ and τ Share One Element. Suppose $\sigma = (a\ b\ c)$ and $\tau = (a\ d)(b\ e)$.

$$\sigma\tau = (a\ b\ c)(a\ d)(b\ e) = (a\ b\ e).$$

In this case, $\sigma\tau$ is a 3-cycle.

Conclusion. The product of a 3-cycle and a product of two disjoint 2-cycles in S_4 is always a 3-cycle.

<div align="right">□</div>

d. H is a Subgroup of S_4.

Proof. Let H be the subset of S_4 consisting of all 3-cycles, all products of disjoint 2-cycles, and the identity.

Closure. We have shown in part (b) that the product of any two 3-cycles is either the identity, a 3-cycle, or a product of two disjoint 2-cycles, and in part (c) that the product of a 3-cycle with a product of two disjoint 2-cycles is a 3-cycle. Since the product of two products of disjoint 2-cycles is also in H, H is closed under the group operation.

Identity. The identity element e is explicitly included in H.

Inverses.

    – The inverse of a 3-cycle $(a\ b\ c)$ is $(a\ c\ b)$, which is also a 3-cycle.

    – The inverse of a product of disjoint 2-cycles $(a\ b)(c\ d)$ is itself, $(a\ b)(c\ d)$.

    – The identity element is its own inverse.

    Since all elements in H have their inverses in H, H contains inverses.

Conclusion. Thus, H is a subgroup of S_4.

<div align="right">□</div>

Exercise 2.2.10. $\Phi(14)$ is cyclic of order 6. Which elements of $\Phi(14)$ are generators? What is the order of each element of $\Phi(14)$?

_____

SOLUTION

To analyze the group $\Phi(14)$, we will identify its structure and determine the generators and the order of each element.

Structure of $\Phi(14)$. The group $\Phi(14)$ is the group of units modulo 14, consisting of integers less than 14 that are coprime to 14. We have:

$$\Phi(14) = \{x \in \mathbb{Z}_{14}^* \mid \gcd(x, 14) = 1\}.$$

Checking each integer from 1 to 13:

- $\gcd(1, 14) = 1 \implies 1 \in \Phi(14)$.
- $\gcd(2, 14) = 2 \implies 2 \notin \Phi(14)$.
- $\gcd(3, 14) = 1 \implies 3 \in \Phi(14)$.
- $\gcd(4, 14) = 2 \implies 4 \notin \Phi(14)$.
- $\gcd(5, 14) = 1 \implies 5 \in \Phi(14)$.
- $\gcd(6, 14) = 2 \implies 6 \notin \Phi(14)$.
- $\gcd(7, 14) = 7 \implies 7 \notin \Phi(14)$.
- $\gcd(8, 14) = 2 \implies 8 \notin \Phi(14)$.
- $\gcd(9, 14) = 1 \implies 9 \in \Phi(14)$.
- $\gcd(10, 14) = 2 \implies 10 \notin \Phi(14)$.
- $\gcd(11, 14) = 1 \implies 11 \in \Phi(14)$.
- $\gcd(12, 14) = 2 \implies 12 \notin \Phi(14)$.
- $\gcd(13, 14) = 1 \implies 13 \in \Phi(14)$.

Thus, the elements of $\Phi(14)$ are:

$$\Phi(14) = \{1, 3, 5, 9, 11, 13\}.$$

Orders of Elements in $\Phi(14)$**.** Since $\Phi(14)$ is cyclic of order 6, the order of an element x in $\Phi(14)$ is the smallest positive integer k such that $x^k \equiv 1 \pmod{14}$.

We compute the orders of each element in $\Phi(14)$:

  – **1**:
$$1^1 \equiv 1 \pmod{14} \implies \text{order of 1 is 1.}$$

  – **3**:
$$3^1 \equiv 3 \pmod{14}, \quad 3^2 \equiv 9 \pmod{14}, \quad 3^3 \equiv 27 \equiv -1 \pmod{14}, \quad 3^6 \equiv (-1)^2 \equiv 1 \pmod{14}.$$
$$\text{Order of 3 is 6.}$$

  – **5**:
$$5^1 \equiv 5 \pmod{14}, \quad 5^2 \equiv 25 \equiv 11 \pmod{14}, \quad 5^3 \equiv 55 \equiv -1 \pmod{14}, \quad 5^6 \equiv (-1)^2 \equiv 1 \pmod{14}.$$
$$\text{Order of 5 is 6.}$$

  – **9**:
$$9^1 \equiv 9 \pmod{14}, \quad 9^2 \equiv 81 \equiv -1 \pmod{14}, \quad 9^3 \equiv (-1) \cdot 9 \equiv 1 \pmod{14}.$$
$$\text{Order of 9 is 3.}$$

  – **11**:
$$11^1 \equiv 11 \pmod{14}, \quad 11^2 \equiv 121 \equiv -1 \pmod{14}, \quad 11^3 \equiv (-1) \cdot 11 \equiv 1 \pmod{14}.$$
$$\text{Order of 11 is 3.}$$

  – **13**:
$$13^1 \equiv 13 \pmod{14}, \quad 13^2 \equiv 169 \equiv 1 \pmod{14}.$$
$$\text{Order of 13 is 2.}$$

Generators of $\Phi(14)$**.** An element g in a cyclic group of order n is a generator if its order is n. Therefore, the generators of $\Phi(14)$ (a cyclic group of order 6) are elements whose order is 6.

$$\text{Generators of } \Phi(14) : \{3, 5\}.$$

Conclusion. The elements of $\Phi(14)$ and their orders are:

Element	Order
1	1
3	6
5	6
9	3
11	3
13	2

The generators of $\Phi(14)$ are $\{3, 5\}$.

Exercise 5. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Show that as elements of the group $GL_2(\mathbb{R})$, the element A has order 4, the element B has order 3, and the element $C := AB$ has infinite order.

SOLUTION

To determine the orders of the matrices A, B, and C in $GL_2(\mathbb{R})$, we will compute their powers and analyze their resulting behavior.

Order of A. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

We compute the powers of A:

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$$

$$A^3 = A^2 \cdot A = (-I) \cdot A = -A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

$$A^4 = A^3 \cdot A = (-A) \cdot A = -A^2 = -(-I) = I.$$

Since $A^4 = I$ and no lower positive power of A equals the identity matrix I, the order of A is:

$$\text{Order of } A = 4.$$

Order of B. Let $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

We compute the powers of B:

$$B^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}.$$

$$B^3 = B^2 \cdot B = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = I.$$

Since $B^3 = I$ and no lower positive power of B equals the identity matrix I, the order of B is:

$$\text{Order of } B = 3.$$

Order of $C := AB$. Let $C = AB$, where $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

We compute C and analyze its powers:

$$C = AB = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Next, we compute the powers of C:

$$C^2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

$$C^3 = C^2 \cdot C = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}.$$

$$C^4 = C^3 \cdot C = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix}.$$

$$C^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

Since C^n does not equal the identity matrix I for any positive integer n, the order of C is:

$$\text{Order of } C = \infty.$$

Conclusion. The orders of the matrices A, B, and C in $GL_2(\mathbb{R})$ are:

Matrix	Order
A	4
B	3
$C = AB$	∞

Exercise 2.2.24. Suppose that a group G of order 20 has at least three elements of order 4. Can G be cyclic? What if G has exactly two elements of order 4?

SOLUTION

To address this problem, we will analyze the structure of a group G of order 20 and investigate the implications of having elements of order 4 on whether G can be cyclic.

Part 1: Can G be cyclic if it has at least three elements of order 4?

Proof.

Let G be a group of order 20. If G is cyclic, then it is generated by a single element, say g, and all its elements are powers of g. The number of elements of each possible order in a cyclic group is determined by the divisors of the group's order.

In a cyclic group of order 20, the possible orders of elements are the divisors of 20, which are 1, 2, 4, 5, 10, and 20.

Counting Elements of Each Order. The number of elements of a given order d in a cyclic group of order n is given by $\phi(d)$, where ϕ is the Euler totient function. We compute the number of elements of each order in a cyclic group of order 20:

Order	Number of Elements
1	$\phi(1) = 1$
2	$\phi(2) = 1$
4	$\phi(4) = 2$
5	$\phi(5) = 4$
10	$\phi(10) = 4$
20	$\phi(20) = 8$

In particular, there are only 2 elements of order 4 in a cyclic group of order 20.

Contradiction. Given that G has at least three elements of order 4, G cannot be cyclic because a cyclic group of order 20 can only have at most 2 elements of order 4. Thus:

If G has at least three elements of order 4, G cannot be cyclic.

$\square$

Part 2: Can G be cyclic if it has exactly two elements of order 4?

Proof.

If G has exactly two elements of order 4, it aligns with the structure of a cyclic group of order 20, where there are indeed 2 elements of order 4.

Verification. In a cyclic group of order 20, generated by an element g, the elements of order 4 are g^5 and g^{15} because:

$$(g^5)^4 = g^{20} = e \quad \text{and} \quad (g^{15})^4 = g^{60} = g^{20 \cdot 3} = e.$$

These are the only two elements of order 4 in a cyclic group of order 20. Thus, having exactly two elements of order 4 is consistent with G being cyclic.

Conclusion. Therefore:

If G has exactly two elements of order 4, G can be cyclic.

$\square$

Summary.

- If G has at least three elements of order 4, G cannot be cyclic.
- If G has exactly two elements of order 4, G can be cyclic.

Exercise 2.3.6. Find a subgroup of D_6 that is isomorphic to D_3.

SOLUTION

To find a subgroup of the dihedral group D_6 (the group of symmetries of a regular hexagon) that is isomorphic to the dihedral group D_3 (the group of symmetries of a triangle), we will examine the structure and elements of D_6 and identify a suitable subgroup.

Structure of D_6. The dihedral group D_6 has order 12 and consists of the symmetries of a regular hexagon. These symmetries include:

- 6 rotations: e (the identity), r (rotation by $60°$), r^2 (rotation by $120°$), r^3 (rotation by $180°$), r^4 (rotation by $240°$), and r^5 (rotation by $300°$).

- 6 reflections: s, sr, sr^2, sr^3, sr^4, and sr^5, where s is a reflection through one of the axes of symmetry of the hexagon.

The multiplication rules in D_6 are:

$$r^6 = e, \quad s^2 = e, \quad sr = r^{-1}s.$$

Structure of D_3. The dihedral group D_3 has order 6 and consists of the symmetries of a triangle. These symmetries include:

- 3 rotations: e (the identity), r' (rotation by $120°$), and r'^2 (rotation by $240°$).

- 3 reflections: s', $s'r'$, and $s'r'^2$, where s' is a reflection through one of the axes of symmetry of the triangle.

The multiplication rules in D_3 are:

$$r'^3 = e, \quad s'^2 = e, \quad s'r' = r'^{-1}s'.$$

Identifying a Subgroup of D_6 Isomorphic to D_3. To find a subgroup of D_6 isomorphic to D_3, we look for a subgroup of D_6 that has order 6 and exhibits the same multiplication structure.

Consider the subgroup $H = \langle r^2, s \rangle$ of D_6. This subgroup is generated by the rotation r^2 (by $120°$) and the reflection s. We will verify that H is isomorphic to D_3.

Generating Elements and Order. The element r^2 has order 3 in D_6:

$$(r^2)^1 = r^2, \quad (r^2)^2 = r^4, \quad (r^2)^3 = r^6 = e.$$

The element s has order 2 in D_6:

$$s^1 = s, \quad s^2 = e.$$

Verification of Structure. We compute the products in H:
$$r^2 \cdot s = sr^{-2}, \quad r^2 \cdot s = sr^4,$$
$$s \cdot r^2 = sr^2, \quad (sr^2)^2 = sr^2 \cdot sr^2 = r^{-2} = r^4 = e.$$

This matches the structure of D_3 with generators r' and s'. Therefore, the subgroup H exhibits the same multiplication rules as D_3.

Conclusion. The subgroup $H = \langle r^2, s \rangle$ of D_6 is isomorphic to D_3. The elements of H are:
$$H = \{e, r^2, r^4, s, sr^2, sr^4\}.$$

Thus:
$$\text{The subgroup } H = \langle r^2, s \rangle \text{ of } D_6 \text{ is isomorphic to } D_3.$$

Exercise 2.3.7. Find a subgroup of D_6 that is isomorphic to the symmetry group of the rectangle.

SOLUTION

To find a subgroup of the dihedral group D_6 that is isomorphic to the symmetry group of the rectangle, we will analyze the structure of D_6 and identify a suitable subgroup.

Structure of D_6. The dihedral group D_6 has order 12 and consists of the symmetries of a regular hexagon. These symmetries include:

- 6 rotations: e (the identity), r (rotation by $60°$), r^2 (rotation by $120°$), r^3 (rotation by $180°$), r^4 (rotation by $240°$), and r^5 (rotation by $300°$).

- 6 reflections: s, sr, sr^2, sr^3, sr^4, and sr^5, where s is a reflection through one of the axes of symmetry of the hexagon.

The multiplication rules in D_6 are:

$$r^6 = e, \quad s^2 = e, \quad sr = r^{-1}s.$$

Structure of the Symmetry Group of the Rectangle. The symmetry group of the rectangle (denoted D_2) has order 4 and consists of the following symmetries:

- 2 rotations: e (the identity), r' (rotation by $180°$).

- 2 reflections: s' (reflection about a horizontal or vertical axis), $r's'$ (reflection about the other axis).

The multiplication rules in D_2 are:

$$r'^2 = e, \quad s'^2 = e, \quad s'r' = r's'.$$

Identifying a Subgroup of D_6 Isomorphic to the Symmetry Group of the Rectangle. We need to find a subgroup of D_6 with order 4 that matches the structure of the symmetry group of the rectangle.

Consider the subgroup $H = \langle r^3, s \rangle$ of D_6. This subgroup is generated by the rotation r^3 (by $180°$) and the reflection s. We will verify that H is isomorphic to D_2.

Generating Elements and Order. The element r^3 has order 2 in D_6:

$$(r^3)^1 = r^3, \quad (r^3)^2 = r^6 = e.$$

The element s has order 2 in D_6:

$$s^1 = s, \quad s^2 = e.$$

Verification of Structure. We compute the products in H:
$$r^3 \cdot s = sr^{-3} = sr^3, \quad s \cdot r^3 = sr^3.$$

This matches the structure of the symmetry group of the rectangle with generators r' and s'.

The elements of H are:
$$H = \{e, r^3, s, sr^3\}.$$

Group Presentation of H.
$$H = \langle r^3, s \mid r^6 = e, s^2 = e, sr = r^{-1}s \rangle \cap \{e, r^3, s, sr^3\}$$

The multiplication rules in H match those of D_2.

Conclusion. The subgroup $H = \langle r^3, s \rangle$ of D_6 is isomorphic to the symmetry group of the rectangle D_2. Thus:

The subgroup $H = \langle r^3, s \rangle$ of D_6 is isomorphic to the symmetry group of the rectangle D_2.