MATH 417, HOMEWORK 8

CHARLES ANCEL

Exercise 2.7.11. Prove that if $G/\mathbb{Z}(G)$ is cyclic, then G is abelian.

Solution

Suppose G is a group such that $G/\mathbb{Z}(G)$ is cyclic. We need to show that G is abelian.

Proof.

Let $G/\mathbb{Z}(G)$ be cyclic. This means there exists an element $g \in G$ such that every element of $G/\mathbb{Z}(G)$ can be written as $g\mathbb{Z}(G)^k$ for some integer k. Hence,

$$G/\mathbb{Z}(G) = \langle g\mathbb{Z}(G)\rangle.$$

Let $x, y \in G$. We need to show that $xy = yx$.

Since $G/\mathbb{Z}(G)$ is cyclic, there exist integers m and n such that

$$x\mathbb{Z}(G) = g^m\mathbb{Z}(G) \quad \text{and} \quad y\mathbb{Z}(G) = g^n\mathbb{Z}(G).$$

This implies:

$$x = g^m z_1 \quad \text{and} \quad y = g^n z_2,$$

for some $z_1, z_2 \in \mathbb{Z}(G)$ (elements of the center of G).

Since elements of the center of a group commute with all elements of the group, we have:

$$xy = (g^m z_1)(g^n z_2) = g^m(z_1 g^n)z_2 = g^m g^n z_1 z_2 = g^{m+n} z_1 z_2.$$

Similarly, we have:

$$yx = (g^n z_2)(g^m z_1) = g^n(z_2 g^m)z_1 = g^n g^m z_2 z_1 = g^{n+m} z_2 z_1.$$

Since multiplication in the center is commutative, we have $z_1 z_2 = z_2 z_1$. Therefore,

$$g^{m+n} z_1 z_2 = g^{n+m} z_2 z_1.$$

Hence,

$$xy = yx.$$

Since x and y were arbitrary elements of G, we conclude that G is abelian.

$\square$

Exercise 2. Recall that for $g \in G$, we write $c_g \in \mathrm{Aut}(G)$ for the automorphism defined by $c_g(x) := gxg^{-1}$. Prove that for any $\phi \in \mathrm{Aut}(G)$ we have $\phi \circ c_g \circ \phi^{-1} = c_{\phi(g)}$. Use this to show that the subgroup $\mathrm{Inn}(G)$ of inner automorphisms is normal in $\mathrm{Aut}(G)$.

Solution

Part 1: Showing $\phi \circ c_g \circ \phi^{-1} = c_{\phi(g)}$. Let $g \in G$ and $\phi \in \mathrm{Aut}(G)$. We want to show that:

$$\phi \circ c_g \circ \phi^{-1} = c_{\phi(g)}.$$

Recall that $c_g(x) = gxg^{-1}$ for all $x \in G$. Let's apply $\phi \circ c_g \circ \phi^{-1}$ to an arbitrary element $x \in G$:

$$(\phi \circ c_g \circ \phi^{-1})(x) = \phi(c_g(\phi^{-1}(x))).$$

By the definition of c_g:

$$c_g(\phi^{-1}(x)) = g\phi^{-1}(x)g^{-1}.$$

Applying ϕ to this result:

$$\phi(g\phi^{-1}(x)g^{-1}) = \phi(g)\phi(\phi^{-1}(x))\phi(g^{-1}).$$

Since ϕ is an automorphism, it is a homomorphism, and thus $\phi(\phi^{-1}(x)) = x$ and $\phi(g^{-1}) = \phi(g)^{-1}$. Therefore:

$$\phi(g)\phi(\phi^{-1}(x))\phi(g^{-1}) = \phi(g)x\phi(g)^{-1}.$$

This is precisely the definition of $c_{\phi(g)}(x)$:

$$c_{\phi(g)}(x) = \phi(g)x\phi(g)^{-1}.$$

Thus, we have shown that:

$$\phi \circ c_g \circ \phi^{-1} = c_{\phi(g)}.$$

Part 2: Showing Inn(G) is Normal in Aut(G). The set of inner automorphisms $\mathrm{Inn}(G)$ is defined as:

$$\mathrm{Inn}(G) = \{c_g \mid g \in G\}.$$

To show that $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$, we need to show that for any $\phi \in \mathrm{Aut}(G)$ and any $c_g \in \mathrm{Inn}(G)$, the conjugate $\phi \circ c_g \circ \phi^{-1}$ is also in $\mathrm{Inn}(G)$.

From Part 1, we have:

$$\phi \circ c_g \circ \phi^{-1} = c_{\phi(g)}.$$

Since $\phi(g) \in G$, it follows that $c_{\phi(g)} \in \mathrm{Inn}(G)$. Thus, $\phi \circ c_g \circ \phi^{-1}$ is an inner automorphism for any $g \in G$ and any $\phi \in \mathrm{Aut}(G)$.

Therefore, $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$.

Exercise 3. Show that $\Phi(15)$ is isomorphic to a product of two of its trivial subgroups.

Solution

Recall that $\Phi(15)$ represents the group of units modulo 15, i.e., $\mathbb{Z}_{15}^*$. The elements of $\mathbb{Z}_{15}^*$ are those integers less than 15 that are coprime to 15. We have:

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\},$$

which has order $\varphi(15) = 8$.

We know that $15 = 3 \times 5$, and since 3 and 5 are coprime, by the Chinese Remainder Theorem (CRT), we have:

$$\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*.$$

Let's explicitly find the isomorphism. The group $\mathbb{Z}_3^*$ is the group of units modulo 3:

$$\mathbb{Z}_3^* = \{1, 2\},$$

which has order 2. The group $\mathbb{Z}_5^*$ is the group of units modulo 5:

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\},$$

which has order 4.

We can construct the isomorphism $\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*$ as follows. For each element $a \in \mathbb{Z}_{15}^*$, we can find its corresponding elements in $\mathbb{Z}_3^*$ and $\mathbb{Z}_5^*$ by considering $a \mod 3$ and $a \mod 5$. This map is given by:

$$a \mapsto (a \mod 3, a \mod 5).$$

Let's verify this mapping for each element in $\mathbb{Z}_{15}^*$:

a	$(a \mod 3, a \mod 5)$
1	$(1, 1)$
2	$(2, 2)$
4	$(1, 4)$
7	$(1, 2)$
8	$(2, 3)$
11	$(2, 1)$
13	$(1, 3)$
14	$(2, 4)$

We observe that each pair $(a \mod 3, a \mod 5)$ is unique and matches the product structure of $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$. Therefore, the mapping:

$$\Phi : \mathbb{Z}_{15}^* \to \mathbb{Z}_3^* \times \mathbb{Z}_5^*, \quad a \mapsto (a \mod 3, a \mod 5)$$

is an isomorphism.

Conclusion. We have shown that $\Phi(15) \cong \mathbb{Z}_{15}^*$ is isomorphic to the product $\mathbb{Z}_3^* \times \mathbb{Z}_5^*$, each of which can be considered trivial subgroups of their respective cyclic groups. Therefore, $\Phi(15)$ is isomorphic to a product of two of its trivial subgroups.

Exercise 3.2.4. Show that the permutation group $S_n (n \geq 2)$ is isomorphic to a semi-direct product of $\mathbb{Z}_2$ and the subgroup A_n of even permutations.

Solution

To show that the symmetric group S_n is isomorphic to a semidirect product of $\mathbb{Z}_2$ and A_n, the alternating group, we need to establish the following:

(1) Identify a subgroup H of S_n isomorphic to A_n.

(2) Identify a normal subgroup N of S_n isomorphic to $\mathbb{Z}_2$.

(3) Show that S_n can be written as a semidirect product $H \rtimes N$.

Subgroup $H \cong A_n$. The alternating group A_n is the subgroup of S_n consisting of all even permutations. This subgroup A_n has order $n!/2$.

Subgroup $N \cong \mathbb{Z}_2$. Consider the subgroup $N = \langle \tau \rangle$, where τ is a transposition (a 2-cycle). For example, $\tau = (1\ 2)$. This subgroup N is isomorphic to $\mathbb{Z}_2$ because:

$$\tau^2 = e,$$

where e is the identity permutation. Thus, $N = \{e, \tau\}$ and τ has order 2.

Semidirect Product Structure. We need to show that $S_n = A_n \rtimes \mathbb{Z}_2$. This means:

(1) $S_n = A_n \cdot \mathbb{Z}_2$.

(2) $A_n \cap \mathbb{Z}_2 = \{e\}$.

(3) The action of $\mathbb{Z}_2$ on A_n is by conjugation.

Proof.

Direct Product. First, we show that every element $\sigma \in S_n$ can be written as a product of an even permutation and an element of $\mathbb{Z}_2$. Consider any permutation $\sigma \in S_n$. If σ is even, then $\sigma \in A_n$. If σ is odd, then σ can be written as $\sigma = \tau\pi$, where τ is a transposition and π is an even permutation. Therefore, $S_n = A_n \cdot \mathbb{Z}_2$.

Intersection. Next, we show that $A_n \cap \mathbb{Z}_2 = \{e\}$. Since A_n consists of even permutations and $\mathbb{Z}_2$ is generated by a single transposition (which is odd), their intersection can only be the identity permutation. Therefore, $A_n \cap \mathbb{Z}_2 = \{e\}$.

Action by Conjugation. Finally, we show that the action of $\mathbb{Z}_2$ on A_n is by conjugation. For any $\sigma \in A_n$ and $\tau \in \mathbb{Z}_2$, we have:

$$\tau\sigma\tau^{-1} = \sigma' \quad \text{for some } \sigma' \in A_n.$$

Since conjugation by a transposition changes the parity of a permutation, σ' will be an even permutation if σ is even. Therefore, the conjugation action of $\mathbb{Z}_2$ on A_n is well-defined.

$\square$

Conclusion. We have shown that S_n can be expressed as a semidirect product of $\mathbb{Z}_2$ and A_n. Thus, we conclude that the permutation group S_n ($n \geq 2$) is isomorphic to a semidirect product of $\mathbb{Z}_2$ and A_n:

$$S_n \cong A_n \rtimes \mathbb{Z}_2.$$

Exercise 5. Consider the semidirect product $G = N \rtimes_\gamma A$, where $N = \langle r \rangle$ is cyclic of order 8, $A = \langle a \rangle$ is cyclic of order 2, and $\gamma : A \to \mathrm{Aut}(N)$ is defined by $\gamma_a(r^k) = r^{3k}$. Determine the orders of each of the elements of G, and show that G is not isomorphic to D_8.

Solution

Element Orders in G. The group N is cyclic of order 8, so $N = \langle r \rangle$ with:

$$r^8 = e_N.$$

The group A is cyclic of order 2, so $A = \langle a \rangle$ with:

$$a^2 = e_A.$$

The semidirect product $G = N \rtimes_\gamma A$ consists of elements (r^k, e_A) and (r^k, a) for $k = 0, 1, \ldots, 7$.

Orders of (r^k, e_A). For (r^k, e_A), we have:

$$(r^k, e_A)^n = (r^k, e_A) \cdot (r^k, e_A) \cdots (r^k, e_A) = (r^{kn}, e_A).$$

Since $r^8 = e_N$, the order of (r^k, e_A) is the smallest n such that $r^{kn} = e_N$. This is:

$$\mathrm{order}((r^k, e_A)) = \frac{8}{\gcd(k, 8)}.$$

Specifically:

- (r^0, e_A): order 1.
- (r^1, e_A): order 8.
- (r^2, e_A): order 4.
- (r^3, e_A): order 8.
- (r^4, e_A): order 2.
- (r^5, e_A): order 8.
- (r^6, e_A): order 4.
- (r^7, e_A): order 8.

Orders of (r^k, a). For (r^k, a), we have:

$$(r^k, a)^2 = (r^k, a) \cdot (r^k, a) = (r^k \gamma_a(r^k), a^2) = (r^k r^{3k}, e_A) = (r^{4k}, e_A).$$

Therefore:

$$(r^k, a)^4 = ((r^{4k}, e_A))^2 = (r^{8k}, e_A) = (e_N, e_A).$$

So the order of (r^k, a) is 4 if k is odd, and 2 if k is even:

- (r^0, a): order 2.
- (r^1, a): order 4.
- (r^2, a): order 2.

- (r^3, a): order 4.
- (r^4, a): order 2.
- (r^5, a): order 4.
- (r^6, a): order 2.
- (r^7, a): order 4.

G is not isomorphic to D_8. The dihedral group D_8 consists of 8 rotations and 8 reflections, where:

$$D_8 = \{e, r, r^2, r^3, r^4, r^5, r^6, r^7, s, sr, sr^2, sr^3, sr^4, sr^5, sr^6, sr^7\},$$

with the relations:

$$r^8 = e, \quad s^2 = e, \quad srs = r^{-1}.$$

Element Orders in D_8. The orders of elements in D_8 are:

- Rotations r^k: order $\frac{8}{\gcd(k,8)}$.
- Reflections sr^k: order 2.

Comparing Orders. We observe that in G, the elements (r^k, a) for odd k have order 4, while in D_8, the reflections sr^k have order 2. Specifically, D_8 does not have elements of order 4 among the reflections.

This difference in element orders implies that G cannot be isomorphic to D_8.

Conclusion. The group $G = N \rtimes_\gamma A$ has elements with orders that do not match those of D_8, specifically the elements (r^k, a) for odd k have order 4 in G, whereas no such elements exist in D_8. Therefore, G is not isomorphic to D_8.

Exercise 6. Let G be the set of bijections $T_{a,b} : \mathbb{R} \to \mathbb{R}$ of the form

$$T_{a,b}(x) := ax + b, \qquad a \in \{\pm 1\}, \qquad b \in \mathbb{Z}$$

(i) Show that G is a group under composition, and that it is generated by the pair of elements

$$r := T_{1,1}, \qquad j := T_{-1,0}$$

which satisfy identities: $j^2 = \mathrm{id}, \quad jr = r^{-1}j$.

(ii) Show that every element of G can be written uniquely in the form:

$$r^a, j^b, \qquad a \in \mathbb{Z},\ b \in \{0, 1\}.$$

(iii) Show that G is isomorphic to a semi-direct product of the form $\mathbb{Z} \rtimes_\gamma \mathbb{Z}_2$, and determine the homomorphism $\gamma : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z})$

Solution

(i) Group Structure of G. To show that G is a group under composition, we need to verify the group axioms: closure, associativity, identity element, and inverses.

Closure. Let $T_{a,b}, T_{c,d} \in G$, where $a, c \in \{\pm 1\}$ and $b, d \in \mathbb{Z}$. The composition $T_{a,b} \circ T_{c,d}$ is given by:

$$(T_{a,b} \circ T_{c,d})(x) = T_{a,b}(T_{c,d}(x)) = T_{a,b}(cx + d) = a(cx + d) + b = acx + ad + b.$$

Since $a, c \in \{\pm 1\}$, we have $ac \in \{\pm 1\}$, and $ad + b \in \mathbb{Z}$. Therefore, $T_{a,b} \circ T_{c,d} = T_{ac,ad+b} \in G$, so G is closed under composition.

Associativity. Composition of functions is always associative.

Identity Element. The identity element in G is the bijection $T_{1,0}$, since:

$$T_{1,0}(x) = 1 \cdot x + 0 = x.$$

For any $T_{a,b} \in G$:

$$T_{1,0} \circ T_{a,b} = T_{a,b} \quad \text{and} \quad T_{a,b} \circ T_{1,0} = T_{a,b}.$$

Inverses. The inverse of $T_{a,b}$ is $T_{a,b}^{-1} = T_{a^{-1},-a^{-1}b}$, where $a^{-1} = a$ since $a \in \{\pm 1\}$. Therefore:

$$T_{a,b} \circ T_{a^{-1},-a^{-1}b} = T_{1,0} \quad \text{and} \quad T_{a^{-1},-a^{-1}b} \circ T_{a,b} = T_{1,0}.$$

This shows that every element in G has an inverse.

Generating Elements and Identities. Consider $r = T_{1,1}$ and $j = T_{-1,0}$:

$$r(x) = x + 1 \quad \text{and} \quad j(x) = -x.$$

Compute j^2:

$$j^2(x) = j(j(x)) = j(-x) = -(-x) = x,$$

which shows $j^2 = \mathrm{id}$.

Compute jr:

$$jr(x) = j(r(x)) = j(x + 1) = -(x + 1) = -x - 1.$$

Compute $r^{-1}j$:

$$r^{-1}(x) = x - 1 \quad \text{and} \quad r^{-1}j(x) = r^{-1}(-x) = -x - 1.$$

Thus, $jr = r^{-1}j$.

(ii) Unique Representation in G. We need to show that every element in G can be written uniquely in the form $r^a j^b$, where $a \in \mathbb{Z}$ and $b \in \{0, 1\}$.

Proof.

Consider an arbitrary element $T_{a,b} \in G$. There are two cases for a:

- $a = 1$:

$$T_{1,b}(x) = x + b = r^b(x).$$

- $a = -1$:

$$T_{-1,b}(x) = -x + b.$$

  We can rewrite $T_{-1,b}(x)$ using j and r:

$$T_{-1,b}(x) = j(x) + b = j(r^b(x)) = jr^b(x).$$

Therefore, every element $T_{a,b} \in G$ can be written as:

$$T_{a,b}(x) = \begin{cases} r^b(x) & \text{if } a = 1, \\ jr^b(x) & \text{if } a = -1. \end{cases}$$

This shows that every element can be written uniquely in the form $r^a j^b$, where $a \in \mathbb{Z}$ and $b \in \{0, 1\}$.

$\square$

(iii) Isomorphism with Semidirect Product $\mathbb{Z} \rtimes_\gamma \mathbb{Z}_2$. To show that G is isomorphic to $\mathbb{Z} \rtimes_\gamma \mathbb{Z}_2$, we need to define the homomorphism $\gamma : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z})$ and verify the isomorphism.

Proof.

Let $\mathbb{Z}_2 = \{0, 1\}$ with addition modulo 2. Define γ by:

$$\gamma_0(a) = a \quad \text{and} \quad \gamma_1(a) = -a.$$

We have:

$$\gamma_0 : \mathbb{Z} \to \mathbb{Z} \quad \text{is the identity automorphism, and}$$
$$\gamma_1 : \mathbb{Z} \to \mathbb{Z} \quad \text{is the automorphism given by negation.}$$

Consider the semidirect product $G = \mathbb{Z} \rtimes_\gamma \mathbb{Z}_2$. The elements of G are pairs (a, b), where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_2$, with the multiplication:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 + \gamma_{b_1}(a_2), b_1 + b_2).$$

The isomorphism $\phi : \mathbb{Z} \rtimes_\gamma \mathbb{Z}_2 \to G$ is defined by:

$$\phi((a, b)) = r^a j^b.$$

Check that ϕ is a homomorphism:

$$\phi((a_1, b_1) \cdot (a_2, b_2)) = \phi((a_1 + \gamma_{b_1}(a_2), b_1 + b_2)) = r^{a_1+\gamma_{b_1}(a_2)} j^{b_1+b_2},$$
$$\phi((a_1, b_1)) \cdot \phi((a_2, b_2)) = (r^{a_1} j^{b_1}) \cdot (r^{a_2} j^{b_2}).$$

Since:

$$j^{b_1} r^{a_2} = r^{\gamma_{b_1}(a_2)} j^{b_1},$$
$$\phi((a_1, b_1)) \cdot \phi((a_2, b_2)) = r^{a_1} r^{\gamma_{b_1}(a_2)} j^{b_1+b_2} = r^{a_1+\gamma_{b_1}(a_2)} j^{b_1+b_2}.$$

Therefore, ϕ is a homomorphism.

Since ϕ is bijective and a homomorphism, it is an isomorphism. Thus, $G \cong \mathbb{Z} \rtimes_\gamma \mathbb{Z}_2$, where $\gamma : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z})$ is defined by $\gamma_0(a) = a$ and $\gamma_1(a) = -a$.

$\square$