

MATH 417, HOMEWORK 4

CHARLES ANCEL

CHAPTER III.14

Exercise 5. Find the order of the given factor group:

$$\frac{(\mathbb{Z}_2 \times \mathbb{Z}_4)}{\langle (1, 1) \rangle}$$

Proof. Let's begin with the group $\mathbb{Z}_2 \times \mathbb{Z}_4$. This is a direct product of two groups: \mathbb{Z}_2 , which has 2 elements, and \mathbb{Z}_4 , which has 4 elements. Consequently, the total number of elements in $\mathbb{Z}_2 \times \mathbb{Z}_4$ is $2 \times 4 = 8$.

Now, consider the cyclic subgroup $\langle (1, 1) \rangle$. By taking successive sums of the element $(1, 1)$, we find that this subgroup consists of the elements $\{(1, 1), (0, 2), (1, 3), (0, 0)\}$. Hence, the order of this subgroup is 4.

The order of the factor group, denoted by $\frac{\mathbb{Z}_2 \times \mathbb{Z}_4}{\langle (1, 1) \rangle}$, is then given by the quotient:

$$\frac{\text{order of } \mathbb{Z}_2 \times \mathbb{Z}_4}{\text{order of } \langle (1, 1) \rangle} = \frac{8}{4} = 2.$$

Therefore, the order of the factor group is 2. □

Exercise 12. Give the order of the element in the factor group.

$$(3, 1) + \langle (1, 1) \rangle \text{ in } \frac{(\mathbb{Z}_4 \times \mathbb{Z}_4)}{\langle (1, 1) \rangle}$$

Proof. To find the order of an element in a factor group, we need to determine how many times we can add the element to itself before we get the identity element of the factor group.

In this case, the element in question is $(3, 1) + \langle (1, 1) \rangle$ in the factor group

$$\frac{\mathbb{Z}_4 \times \mathbb{Z}_4}{\langle (1, 1) \rangle}$$

Here, $\mathbb{Z}_4 \times \mathbb{Z}_4$ is the direct product of the group of integers modulo 4. The identity element is $(0, 0)$.

To find the order of $(3, 1) + \langle (1, 1) \rangle$, we'll compute:

(1) $(3, 1) + (3, 1)$

(2) $(3, 1) + (3, 1) + (3, 1)$

$$(3) \quad (3, 1) + (3, 1) + (3, 1) + (3, 1)$$

... and so on, until we get an element of the subgroup $\langle(1, 1)\rangle$, which represents the identity of the factor group.

The element $(3, 1) + \langle(1, 1)\rangle$ has order 2 in the factor group $\frac{\mathbb{Z}_4 \times \mathbb{Z}_4}{\langle(1, 1)\rangle}$.

In the group $\mathbb{Z}_4 \times \mathbb{Z}_4$: 1. $(3, 1) + (3, 1) = (2, 2)$

Since $(2, 2)$ is an element of the subgroup $\langle(1, 1)\rangle$, and the subgroup represents the identity in the factor group, we conclude that the element $(3, 1) + \langle(1, 1)\rangle$ has order 2 in the factor group. \square

Exercise 24. Show that A_n is a normal subgroup of S_n and compute $\frac{S_n}{A_n}$; that is, find a known group to which $\frac{S_n}{A_n}$ is isomorphic.

Proof.

1. **Showing A_n is a normal subgroup of S_n :**

Recall that A_n is the group of even permutations in S_n , and it consists of all permutations that can be expressed as a product of an even number of transpositions. The order of A_n is half the order of S_n , i.e., $|A_n| = \frac{n!}{2}$.

Let σ be an element in S_n and τ be an element in A_n . If we conjugate τ by σ , we get $\sigma\tau\sigma^{-1}$. The number of transpositions in $\sigma\tau\sigma^{-1}$ is even since both σ and σ^{-1} either add an even number of transpositions or do not change the number of transpositions in τ . Thus, $\sigma\tau\sigma^{-1}$ is an even permutation, which means it lies in A_n .

Since this is true for any σ in S_n and any τ in A_n , A_n is invariant under conjugation by elements of S_n . Hence, A_n is a normal subgroup of S_n .

2. **Computing $\frac{S_n}{A_n}$:**

Since $|S_n| = n!$ and $|A_n| = \frac{n!}{2}$, the factor group $\frac{S_n}{A_n}$ has order 2. Any group of order 2 is isomorphic to \mathbb{Z}_2 (the group of integers modulo 2).

Specifically, the factor group $\frac{S_n}{A_n}$ consists of two cosets: A_n itself and the set of all odd permutations. These two cosets can be identified with the elements 0 and 1 in \mathbb{Z}_2 , respectively.

Therefore, $\frac{S_n}{A_n}$ is isomorphic to \mathbb{Z}_2 . \square

Exercise 32. Given any subset S of a group G , show that it makes sense to speak of the smallest normal subgroup that contains S .

Proof. Let's consider the collection of all normal subgroups of G that contain S . We know that G itself is a normal subgroup that contains S , so this collection is nonempty.

Given any family of normal subgroups, their intersection is also a normal subgroup. To see this, let $\{N_i\}$ be a family of normal subgroups of G . For any $g \in G$ and n in the intersection of all N_i , $gn^{-1}g^{-1}$ is in each N_i since each N_i is normal. Therefore, $gn^{-1}g^{-1}$ is in their intersection, and thus their intersection is a normal subgroup.

Now, take the intersection N of all normal subgroups of G that contain S . By the property above, N is also a normal subgroup of G , and $S \subseteq N$ by definition.

For any normal subgroup N' of G that contains S , N' is one of the subgroups we intersected to get N . Hence, $N \subseteq N'$. This means that N is contained in every normal subgroup that contains S , making N the "smallest" such subgroup.

Therefore, it makes sense to speak of the smallest normal subgroup of G that contains S . \square

Exercise 34. Show that if a finite group G has exactly one subgroup H of a given order, then H is a normal subgroup of G .

Proof. Let G be a finite group, and let H be the unique subgroup of G of a given order. Let a be an element of G .

We need to show that for every element a in G , the left coset aH is equal to the right coset Ha , which would imply that H is a normal subgroup of G .

Consider the left coset aH . Since the operation in the group is associative, the set aH is also a subgroup of G . Furthermore, since H is the only subgroup of G of its order and $|aH| = |H|$, it follows that $aH = H$.

Similarly, considering the right coset Ha , we can conclude that $Ha = H$ since $|Ha| = |H|$ and H is the unique subgroup of its order.

Thus, $aH = H = Ha$ for every element a in G , which implies that H is a normal subgroup of G . \square

Exercise 35. Show that if H and N are subgroups of a group G , and N is normal in G , then $H \cap N$ is normal in H .

Proof. Let h be an element of H and x be an element of $H \cap N$.

We want to show that hx and xh are in the same set, which would mean $h(H \cap N) = (H \cap N)h$.

Since x is in N and N is normal in G , hx and xh are both in N .

Furthermore, since h and x are both in H , both hx and xh are in H .

Therefore, hx and xh are both in $H \cap N$.

This shows that for every element h in H , the left coset $h(H \cap N)$ is equal to the right coset $(H \cap N)h$ in H . Hence, $H \cap N$ is a normal subgroup of H . \square

Exercise 38. Show that the set of all $g \in G$ such that $i_g : G \rightarrow G$ is the identity inner automorphism i_e is a normal subgroup of a group G . Let's denote this set by N , i.e.,

$$N = \{g \in G \mid i_g(x) = x \text{ for all } x \in G\}$$

To prove that N is a normal subgroup of G , we'll demonstrate: 1. N is a subgroup of G . 2. N is normal in G .

Proof.

1. N is a subgroup of G :

- **Identity:** The inner automorphism corresponding to the identity element e of G is the identity map, i.e., $i_e(x) = exe^{-1} = x$ for all $x \in G$. Hence, $e \in N$.

- **Closure:** Let $g, h \in N$. For any $x \in G$, we have

$$i_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1}$$

Since $h \in N$, $h x h^{-1} = x$. So, $i_{gh}(x) = g x g^{-1}$. And as $g \in N$, $g x g^{-1} = x$. Hence, $gh \in N$.

- **Inverse:** Let $g \in N$. For any $x \in G$, we have $g x g^{-1} = x$. Multiplying on the right by g and on the left by g^{-1} , we get $x = g^{-1} x g$, which means $i_{g^{-1}}(x) = x$ for all $x \in G$. So, $g^{-1} \in N$.

2. N is normal in G :

Let $g \in N$ and $a \in G$. We need to show that $a^{-1}ga \in N$. For any $x \in G$,

$$i_{a^{-1}ga}(x) = a^{-1}ga x (a^{-1}ga)^{-1} = a^{-1}ga x g^{-1}a^{-1}$$

Since $g \in N$, $ga x g^{-1} = ax$, and thus $i_{a^{-1}ga}(x) = a^{-1}ax = x$. This means $a^{-1}ga \in N$.

Hence, combining the above results, N is a normal subgroup of G .

□

Exercise 40. Use the properties of $\det(AB) = \det(A) \det(B)$ and $\det(I_n) = 1$ for all $n \times n$ matrices to show the following:

(a.) The $n \times n$ matrices with 1 form a normal subgroup of $GL(n, \mathbb{R})$.

(b.) The $n \times n$ matrices with ± 1 form a normal subgroup of $GL(n, \mathbb{R})$.

(a) First, we want to show that the $n \times n$ matrices with determinant 1 form a normal subgroup of $GL(n, \mathbb{R})$. $GL(n, \mathbb{R})$ is the group of $n \times n$ invertible matrices under matrix multiplication.

Let's denote the set of all $n \times n$ matrices with determinant 1 as H .

(a) *Proof.* 1. **H is a subgroup of $GL(n, \mathbb{R})$:**

- **Identity:** The identity matrix I_n has $\det(I_n) = 1$. Hence, $I_n \in H$.
- **Closure:** Let $A, B \in H$. Then, $\det(AB) = \det(A) \times \det(B) = 1 \times 1 = 1$. Thus, $AB \in H$.
- **Inverse:** If $A \in H$, then $\det(A^{-1}) = \frac{1}{\det(A)} = 1$. Hence, $A^{-1} \in H$.

2. **H is normal in $GL(n, \mathbb{R})$:**

Let $A \in H$ and $B \in GL(n, \mathbb{R})$. We need to show that $B^{-1}AB \in H$. Using properties of the determinant, we have:

$$\det(B^{-1}AB) = \det(B^{-1}) \times \det(A) \times \det(B) = \frac{1}{\det(B)} \times 1 \times \det(B) = 1$$

Thus, $B^{-1}AB \in H$.

Hence, the $n \times n$ matrices with determinant 1 form a normal subgroup of $GL(n, \mathbb{R})$.

□

(b) Next, we want to show that the $n \times n$ matrices with determinant ± 1 form a normal subgroup of $GL(n, \mathbb{R})$.

Let's denote the set of all $n \times n$ matrices with determinant ± 1 as K .

(b) *Proof.* 1. **K is a subgroup of $GL(n, \mathbb{R})$:**

- **Identity:** $\det(I_n) = 1$, so $I_n \in K$.
- **Closure:** If $A, B \in K$, then $\det(AB)$ can be 1, -1 , -1 , or 1 respectively based on the determinants of A and B . In all cases, $\det(AB)$ is ± 1 . Thus, $AB \in K$.
- **Inverse:** For $A \in K$, $\det(A^{-1})$ is either 1 or -1 based on $\det(A)$. Hence, $A^{-1} \in K$.

2. **K is normal in $GL(n, \mathbb{R})$:**

Let $A \in K$ and $B \in GL(n, \mathbb{R})$. We need to show that $B^{-1}AB \in K$. From properties of the determinant:

$$\det(B^{-1}AB) = \det(B^{-1}) \times \det(A) \times \det(B)$$

The result will be ± 1 since all factors have determinants of ± 1 . Thus, $B^{-1}AB \in K$.

Hence, the $n \times n$ matrices with determinant ± 1 form a normal subgroup of $GL(n, \mathbb{R})$.

□

CHAPTER III.15

Exercise 17. The *center* of a group G contains all elements of G that commute with every element of G .

To verify the definition of the center of a group G , consider:

$$Z(G) = \{x \in G \mid \forall g \in G, xg = gx\}$$

Proof.

(1) $Z(G)$ is a subgroup of G :

- **Identity:** For any $g \in G$, $eg = ge$, so $e \in Z(G)$.
- **Closure:** For $a, b \in Z(G)$ and any $g \in G$, $(ab)g = a(bg) = a(gb) = (ga)b = g(ab)$. Thus, $ab \in Z(G)$.
- **Inverse:** If $a \in Z(G)$ and any $g \in G$, $a^{-1}g = g(a^{-1})$. Hence, $a^{-1} \in Z(G)$.

(2) $Z(G)$ is **Abelian**: By definition, every element in $Z(G)$ commutes with every element in G , making $Z(G)$ Abelian.

Given that $Z(G)$ is a subgroup of G and is Abelian, the definition provided for the center of a group is accurate. \square

Exercise 28. Give an example of a group G having no elements of finite order > 1 but having a factor group G/H , all of whose elements are of finite order.

Let's consider the group $G = \mathbb{R}/$ under addition and the subgroup $H = \mathbb{Z}$.

- (1) Every non-zero element of $\mathbb{R}/$ has infinite order.
- (2) The factor group $G/H = \mathbb{R}/\mathbb{Z}$ can be thought of as the set of equivalence classes of real numbers modulo 1 (i.e., fractions in the interval $[0,1)$).

Now, let's prove that all elements of \mathbb{R}/\mathbb{Z} have finite order.

Proof. Consider an element $[x]$ in \mathbb{R}/\mathbb{Z} , where $[x]$ denotes the equivalence class of x modulo 1.

For any integer n , the sum of n copies of $[x]$ in \mathbb{R}/\mathbb{Z} is $[nx]$. If nx is an integer, then $[nx]$ is the identity element of \mathbb{R}/\mathbb{Z} , which is $[0]$.

Choose n to be the smallest positive integer such that nx is an integer. Such an n exists because x is a fraction and can be expressed in the form $\frac{p}{q}$, where p and q are coprime integers. In this case, $q \times \frac{p}{q} = p$ is an integer.

Thus, the order of $[x]$ in \mathbb{R}/\mathbb{Z} is finite, and specifically, it is n .

Since $[x]$ was an arbitrary element of \mathbb{R}/\mathbb{Z} , it follows that all elements of \mathbb{R}/\mathbb{Z} have finite order. \square

Exercise 29. Let H and K be normal subgroups of a group G . Give an example showing that we may have $H \equiv K$ while G/H is not isomorphic to G/K .

To construct an example, consider the group $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ (direct product of cyclic groups). Let H be the subgroup generated by $(2, 1)$ and K be the subgroup generated by $(0, 1)$.

Both H and K are isomorphic to \mathbb{Z}_2 , and hence $H \equiv K$.

However, G/H and G/K are not isomorphic. Let's see why:

Proof.

(1) **Structure of G/H :** The cosets of H in G are:

$$H, (1, 0) + H, (2, 0) + H, (3, 0) + H$$

Thus, G/H is isomorphic to \mathbb{Z}_4 .

(2) **Structure of G/K :** The cosets of K in G are:

$$K, (1, 0) + K, (2, 0) + K, (3, 0) + K$$

However, since $(1, 0) + K$ and $(3, 0) + K$ each have an element of order 4, G/K is not isomorphic to \mathbb{Z}_4 . In fact, G/K is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

From the above observations, G/H (isomorphic to \mathbb{Z}_4) is not isomorphic to G/K (isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$), even though $H \equiv K$. \square

Exercise 35. Let $\phi : G \rightarrow G'$ be a group homomorphism, and let N be a normal subgroup of G . Show that $\phi[N]$ is a normal subgroup of $\phi[G]$.

To prove this, let's recall some properties of group homomorphisms:

Given a group homomorphism $\phi : G \rightarrow G'$:

(1) If H is a subgroup of G , then $\phi[H]$ is a subgroup of G' .

(2) $\phi(e) = e'$, where e is the identity of G and e' is the identity of G' .

Given these properties, let's prove that $\phi[N]$ is a normal subgroup of $\phi[G]$.

Proof.

(1) $\phi[N]$ **is a subgroup of** $\phi[G]$:

Since N is a subgroup of G , $\phi[N]$ is a subgroup of $\phi[G]$ (from property 1).

(2) $\phi[N]$ **is normal in** $\phi[G]$:

Let's take any element a' in $\phi[G]$ and any element n' in $\phi[N]$. By the definition of $\phi[G]$ and $\phi[N]$, there exist elements a in G and n in N such that $\phi(a) = a'$ and $\phi(n) = n'$.

Now, consider the conjugation in G' :

$$a'n'a'^{-1} = \phi(a)\phi(n)\phi(a)^{-1}$$

Since ϕ is a homomorphism, this is equal to:

$$\phi(ana^{-1})$$

Now, because N is normal in G , the element ana^{-1} is in N . Hence, $\phi(ana^{-1})$ is in $\phi[N]$.

This means that the conjugation of any element in $\phi[N]$ by any element in $\phi[G]$ is still in $\phi[N]$, which implies that $\phi[N]$ is normal in $\phi[G]$.

□