6 The Three Isomorphism Theorems

If G and H are groups and $\phi : G \to H$ is a homomorphism with kernel $\mathcal{K}$, we know from Proposition 5.2.4 that $\mathcal{K} \trianglelefteq G$; therefore $G/\mathcal{K}$ is a group by Definition 5.1.1. Recall that, $G/\mathcal{K} = \{g\mathcal{K} : g \in G\}$.

Theorem 6.0.1. (The First Isomorphism Theorem) *Let G and H be groups and let $\phi : G \to H$ be a homomorphism with kernel $\mathcal{K}$ and image $\mathcal{I}$. Then,*

$$G \,/\, \mathcal{K} \cong \mathcal{I}.$$

The isomorphism is the map $\theta : G/\mathcal{K} \to \mathcal{I}$ given by $\theta(g\mathcal{K}) = \phi(g)$.

Proof. We must first check that:

(i) θ is a function (i.e. if $g_1\mathcal{K} = g_2\mathcal{K}$, then we must show that $\theta(g_1\mathcal{K}) = \theta(g_2\mathcal{K})$ because a function can't map the same thing to two different things. (This is called being *well-defined*).

Proof: if $g_1\mathcal{K} = g_2\mathcal{K}$, then $g_1^{-1}g_2 \in \mathcal{K}$ by Theorem 4.1.3, and so $\phi(g_1^{-1}g_2) = e_H$. Since ϕ is a homomorphism, this implies that $\phi(g_1) = \phi(g_2)$. Hence $\theta(g_1\mathcal{K}) = \theta(g_2\mathcal{K})$, so θ is well-defined.

(ii) θ is a homomorphism.

Proof: This is easy. Indeed, $\theta((g_1\mathcal{K})(g_2\mathcal{K})) = \theta((g_1g_2)\mathcal{K}) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \theta((g_1\mathcal{K})\theta((g_2\mathcal{K})$.

(iii) θ is onto.

Proof: This is easy. Indeed, any element in $\mathcal{I}$ is of the form $\phi(g)$ for some $g \in G$, and is therefore equal to $\theta(g\mathcal{K})$.

(iv) θ is one-to-one.

Proof: $\theta(g_1\mathcal{K}) = \theta(g_2\mathcal{K}) \implies \phi(g_1) = \phi(g_2) \implies \phi(g_1^{-1}g_2) = e_H \implies g_1^{-1}g_2 \in \mathcal{K}$. But $g_1^{-1}g_2 \in \mathcal{K}$ implies (by Theorem 4.1.3) that $g_1\mathcal{K} = g_2\mathcal{K}$.

□

Definition 6.0.2. Let G be a group with $N \trianglelefteq G$. The map $\pi : G \to G/N$ given by $\pi(g) = gN$ is a homomorphism (exercise - check this) and obviously has kernel N and image G/N. It is often called the *canonical homomorphism*.

Example 6.0.3. Fix $n \in \mathbb{N}$. Recall Example 5.2.2, where we proved the map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\varphi(m) = [m]_n$ is a homomorphism. We also proved:

- $\mathrm{Ker}(\varphi) = \mathrm{n}\mathbb{Z}$ = the set of multiples of n
- $\mathrm{Im}(\varphi) = \mathbb{Z}_{\mathrm{n}}$.

Using the First Isomorphism Theorem we can deduce that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. We already proved this directly in Example 5.1.2 for $n = 3$. Now we see this phenomena is true for all $n \in \mathbb{N}$.

Theorem 6.0.4. (The Second Isomorphism Theorem) *Let G be a group with $H \leq G$ and $N \trianglelefteq G$. Then the following quotient groups are isomorphic:*

$$H/(H \cap N) \cong (HN)/N.$$

The next theorem is sometimes called "The Fool's Cancellation Theorem" because it looks like the groups can be "cancelled" like integers.

Theorem 6.0.5. (The Third Isomorphism Theorem) *Let G be a group with $N \trianglelefteq G$. If $M \trianglelefteq G$ and $N \leq M \leq G$, then $M/N \trianglelefteq G/N$ and the following quotient groups are isomorphic:*

$$(G/N)/(M/N) \cong G/M.$$

6.0.1 Handout for Section 6

Proof of The Second Isomorphism Theorem. Let $\phi : H \to (HN)/N$ be the map given by $\phi(h) = hN$.

(i) It is easy to prove that this is a homomorphism.

(ii) The kernel is $\mathcal{K} = \{h \in H : hN = e_{HN/N}\} = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N$.

(iii) The image is $\mathcal{I} = \{hN \in (HN)/N : h \in H\} = \{hkN \in (HN)/N : h \in H, k \in N\} = (HN)/N$.

(iv) Result follows immediately from the First Isomorphism Theorem.

$\square$

Proof of the Third Isomorphism Theorem. Let $\phi : G/N \to G/M$ be the map given by $\phi(gN) = gM$.

(i) It is easy to prove this is a homomorphism.

(ii) The kernel is $\mathcal{K} = \{hN : hM = M\} = \{hN : h \in M\} = M/N$.

(iii) The image is $\mathcal{I} = \{gM : gN \in G/N\} = \{gM : g \in G\} = G/M$.

(iv) Result follows immediately from the First Isomorphism Theorem.

$\square$

7 A new permutation group: the alternating group

7.1 Cycle shape

In this section we will define an important homomorphism (called the signature function) on S_n. The kernel of this function is called the *alternating group* and is one of the most important groups in the course—we will explore this group in the next section. Before defining the signature function, we first introduce *cycle shape*. In the next section we will see how to use the cycle shapes to quickly calculate the signature function.

Definition 7.1.1. The *cycle shape* of a permutation just tells you how long its cycles are when written as a product of disjoint cycles. Formally, let $g \in S_n$ be a permutation that is not the identity. We can write g as a product of disjoint cycles,

$$g = c_1 c_2 \cdots c_m,$$

where each cycle c_i has length r_i and $r_1 \geq r_2 \geq \cdots \geq r_m$. The cycle shape of g is then $(r_1, r_2, \dots, r_m)$.

The cycle shape of the identity is usually taken to be $\varnothing$.

Example 7.1.2. Here are some examples of cycle shape.

1. The cycle shape of $g = (1\ 3\ 5\ 7\ 2\ 9)(4\ 8)(10\ 6\ 12\ 11) \in S_{12}$ is $(6,4,2)$ because g is comprised of a cycle of length 6, another of length 4 and one of length 2.

   (Notice that we reordered the cycles before describing the shape.)
2. The cycle shape of $h = (1\ 2)(3\ 4)(7\ 8)(9\ 10) \in S_{10}$ is $(2,2,2,2)$

Question 7.1.3. What are all the cycle shapes that occur in S_4?

For any permutation in S_4 (written as a product of disjoint cycles) we have that each number in $\{1,2,3,4\}$ lies in precisely one cycle (possible a cycle of length one).

Cycle shape	List of elements in S_4 with this cycle shape	No. elements
$\varnothing$	e	1
(2)	$(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $(2\ 3)$, $(2\ 4)$, $(3\ 4)$	6
$(2,2)$	$(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$	3
(3)	$(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$, $(2\ 4\ 3)$	8
(4)	$(1\ 2\ 3\ 4)$, $(1\ 2\ 4\ 3)$, $(1\ 3\ 2\ 4)$, $(1\ 3\ 4\ 2)$, $(1\ 4\ 2\ 3)$, $(1\ 4\ 3\ 2)$	6

We have definitely found everything because $|S_4| = 4! = 24$.