

# VIII. Quotient Groups and Homomorphism Theorems

## 1 Quotient Groups

**Theorem 1.1** : Suppose  $N$  is a normal subgroup of  $G$ . Let  $G/N$  be the collection  $\{aN : a \in G\}$  of all left cosets of  $N$  in  $G$ . Then the binary operation  $(aN) * (bN) := (ab)N$  makes  $G/N$  a group and the function  $f(a) = aN$  is a homomorphism from  $G$  onto  $G/N$ .

**Warning:** Remember that the members of  $G/N$  are equivalence classes and that it can happen that  $aN = a'N$  even though  $a \neq a'$ . Consequently we must worry about whether the proposed group operation on  $G/N$  is well-defined and this is the hardest part of the proof,

Proof: We must show that if  $aN = bN$  and  $cN = dN$  then  $acN = bdN$ . Let's prove a preliminary lemma that is about half of what we want:

**Lemma 1.2** : Suppose  $N$  is a normal subgroup of  $G$  and  $aN = bN$ . Then for any  $c \in G$ ,  $acN = bcN$ .

Proof of Lemma: We will show that the cosets  $(ab)N$  and  $(ac)N$  have something in common and therefore must be identical. From  $aN = bN$  we know that  $a = a * e \in aN = bN$  so that for some  $x \in N$  we have  $a = bx$ . Then  $ac = bxc$ . Consider  $xc$ . Because  $N$  is normal, we know that  $xc \in Nc = cN$  and so there is some  $y \in N$  with  $xc = cy$ . Therefore  $ac = bxc = b(cy) = (bc)y \in (bc)N$ . At this point we know that  $ac \in acN$  and  $ac \in bcN$  so that  $acN \cap bcN \neq \emptyset$ . Therefore,  $acN = bcN$ .  $\square$

We now return to the proof of our proposition. From  $aN = bN$  we know that  $acN = bcN$ . There is an analog of Lemma 1.2 saying that because  $cN = dN$  we know that  $bcN = bdN$ . Therefore we have  $acN = bcN = bdN$  as required.  $\square$

**Homework:** Prove that if  $N$  is a normal subgroup and  $cN = dN$  then for any  $b \in G$ ,  $bcN = bdN$ .

Now that we know that the proposed operation is well-defined, other properties are easy to check.

Associativity:  $((aN)(bN))(cN) = (abN)(cN) = ((ab)c)N = a(bc)N = (aN) * (bN * cN)$ .

identity:  $eN$  acts as the identity in  $G/N$ .

inverses: for each  $aN \in G/N$  we know that  $a^{-1}N \in G/N$  and  $aN * a^{-1}N = eN$ .  $\square$

**Definition:** If  $N$  is a normal subgroup of  $G$ , then the collection of cosets  $G/N := \{aN : a \in G\}$  with the group operation defined above is called the quotient group (or the factor group) of  $G$  modulo  $N$ .

**Proposition 1.3** : Let  $N$  be a normal subgroup of  $G$ . Then the function  $\pi : G \rightarrow G/N$  given by  $\pi(a) = aN$  for every  $a \in G$  is a homomorphism from  $G$  onto  $G/N$ .

Proof: Because we are not using aliases in the domain of  $\pi$  to define  $\pi(x)$ , there is no question about  $\pi$  being well-defined. The function  $\pi$  is onto because for each coset  $aN \in G/N$  we have  $\pi(a) = aN$ . The function  $\pi$  is a homomorphism because  $\pi(ab) = (ab)N = (aN) * (bN) = \pi(a) * \pi(b)$ .  $\square$

**Example 1.4 :** Use addition as the group operation on  $\mathbb{Z}$ , and let  $E$  be the subgroup of all even integers. Then  $\mathbb{Z}/E$  is  $\mathbb{Z}_2$ . Once again using addition as the operation,  $\mathbb{R}/\mathbb{Z}$  is isomorphic to the unit circle  $T := \{z \in \mathbb{C} : ||z|| = 1\}$  in the complex plane, where the group operation on  $T$  is multiplication.

Proof: The group  $\mathbb{Z}/E$  has exactly two members, so it must be  $\mathbb{Z}_2$ . The members of  $\mathbb{R}/\mathbb{Z}$  have the form  $x + \mathbb{Z}$  where  $x \in \mathbb{R}$ . We define a function  $f$  by the rule that  $f(x + \mathbb{Z}) = \cos(2\pi x) + i \sin(2\pi x)$ . This is a well-defined isomorphism from  $(\mathbb{R}/\mathbb{Z}, +)$  onto  $(T, *)$ .  $\square$

**Homework:** Prove that in the previous example,  $f$  is well defined and is an isomorphism onto  $(T, *)$ .

## 2 The Fundamental Homomorphism Theorem

**Question:** Starting with a given group  $G$ , how can we find all groups  $H$  such that there is a homomorphism  $f : G \rightarrow H$  from  $G$  onto  $H$ ?

**Answer:** We use quotient groups  $G/N$  where  $N$  is allowed to be any normal subgroup of  $G$ , as can be seen from the next theorem, known as the *Fundamental Homomorphism Theorem*.

**Theorem 2.1 :** Suppose  $f : G \rightarrow H$  is a homomorphism from  $G$  onto  $H$ . Let  $K := \ker(f)$ . Then  $K$  is a normal subgroup of  $G$  and the quotient group  $G/K$  is isomorphic to  $H$  using the function  $F : G/K \rightarrow H$  given by the rule  $F(aK) := f(a)$ .

Proof: Because aliases of equivalence classes are used to define  $F$  in the statement of our theorem, we must worry about whether  $F$  is well-defined. So suppose  $aK = bK$  where  $K = \ker(f)$ . Then  $a^{-1}b \in K$  so that  $e_H = f(a^{-1}b) = (f(a))^{-1} * f(b)$ . But then in  $H$  we have  $f(a) = f(b)$  so that  $F(aK) = F(bK)$ . Hence  $F$  is well-defined.

Next let  $aK, bK \in G/K$  and observe that  $F(aK * bK) = F((ab)K) = f(ab) = f(a) * f(b) = F(aK) * F(bK)$ . Hence  $F$  is a homomorphism.

Third,  $F$  is onto. Let  $y \in H$ . Because  $f$  is onto, there is some  $a \in G$  with  $y = f(a)$ . But then  $F(aK) = f(a) = y$ , showing that  $F$  is onto.

Finally,  $F$  is 1-1. We will show that  $\ker(F)$  is the subgroup  $\{eK\}$  of  $G/K$ . Clearly  $eK \in \ker(F)$ , so suppose we have  $xK \in \ker(F)$ . Then  $e_H = F(xK) = f(x)$ , showing that  $x \in \ker(f) = K$ . But then  $xK = eK$ . Therefore,  $\ker(F) = \{eK\}$ .  $\square$

**Corollary 2.2 :** There is a homomorphism from  $\mathbb{Z}$  onto the group  $H$  if and only if  $H$  is isomorphic to  $\mathbb{Z}$  or is isomorphic to one of the groups  $\mathbb{Z}_n$ .

### 3 The Converse of Lagrange's Theorem is False

Recall that Lagrange proved that if  $H$  is a subgroup of a finite group  $G$ , then  $|H|$  is a divisor of  $|G|$ . So far we know that the converse is true for Abelian groups, but we do not know what happens in the non-Abelian case. After the next example, we will know.

**Example 3.1** : *The converse of Lagrange's theorem is false. The group  $A_4$  has order 12, but has no subgroup of order 6.*

Proof: We proved that exactly half of all permutations of any finite set are even, so we know that  $|A_n| = \frac{n!}{2}$ . Hence  $A_4$  has order 12. For contradiction, suppose that  $H$  is a subgroup of  $A_4$  having order 6. Then the index of  $H$  in  $A_4$  is 2, i.e.,  $H$  has exactly two cosets in  $A_4$ . According to a homework problem, we know that the two left cosets of  $H$  must be  $H$  and  $aH$ , where  $a$  is any fixed element of  $A_4 - H$ . Similarly the two right cosets are  $H$  and  $Ha$  where  $a \in A_4 - H$  and it follows that  $aH = Ha$  for each  $a \in A_4$ . Hence  $H$  must be a normal subgroup of  $A_4$ .

Construct the factor group  $A_4/H$ . Being a two-element group, it is Abelian (remember that any group of order less than or equal to 5 is Abelian). Furthermore, for each  $a \in A_4$  we know that  $aH$  must be its own inverse in the group  $A_4/H$ , i.e.,  $eH = (aH)^2 = a^2H$ . Therefore, in  $A_4$  we have  $a^2 \in H$  for every  $a \in A_4$ .

At this point we begin using the fact that members of  $A_4$  are even permutations of the set  $\{1, 2, 3, 4\}$ . By computing  $(1, 2, 3)(x)$  and  $(1, 3, 2)^2(x)$  for  $x = 1, 2, 3, 4$  we see that  $(1, 2, 3) = (1, 3, 2)^2$  so that  $(1, 2, 3) \in A_4$  and  $(1, 2, 3) \in H$ . Similarly  $(2, 3, 4) = (2, 4, 3)^2$  so that  $(2, 3, 4) \in H$ . In fact, for any choice of three distinct elements  $r, s, t \in \{1, 2, 3, 4\}$  we have  $(r, s, t) = (r, t, s)^2$  and so we know that  $(r, s, t) \in A_4$  and  $(r, s, t) \in H$ . But then the following are distinct elements of  $H$ :

$$(1, 2, 3); (1, 3, 2); (1, 2, 4); (1, 4, 2); (1, 3, 4); (1, 4, 3); (2, 3, 4); (2, 4, 3)$$

so that  $H$  must have more than six elements, and that is impossible.  $\square$