

## 14. FACTOR GROUPS

Factor groups are an example of the creative side of mathematics. Out of a group  $G$  and a normal subgroup  $N$  we make a new group  $G/N$ . We call this a “construction.”

If  $N \triangleleft G$  then the set of cosets of  $N$  form a group with multiplication defined by

$$(aN)(bN) := abN$$

The additive notation is:

$$(a + N) + (b + N) := (a + b) + N$$

This group, whose elements are the cosets of  $N$  with operation defined by one of the two formulas above, is denoted  $G/N$ . To check that this is a group the only thing we have to check is that the multiplication is “well-defined” because the other conditions are obvious. (E.g.,  $eN = N$  is the identity,  $(aN)^{-1} = a^{-1}N$ .)

*Well-defined* means *independent of all choices*. But what choices did we make?

As I pointed out before, you get the same left coset in many ways.

$$a_1N = a_2N \iff a_1^{-1}a_2 \in N$$

So, suppose that  $a_1N = a_2N$  and  $b_1N = b_2N$ . Then we have two different formulas for the product and we need to show:

$$a_1b_1N = a_2b_2N$$

In other words, we need to check that  $(a_1b_1)^{-1}a_2b_2 \in N$ . But:

$$(a_1b_1)^{-1}a_2b_2 = b_1^{-1}a_1^{-1}a_2b_2 = b_1^{-1}(a_1^{-1}a_2)b_1(b_1^{-1}b_2) \in b_1^{-1}Nb_1N = NN = N$$

**Theorem 14.1.** *If  $N$  is a normal subgroup of a group  $G$  then the set  $G/N$  of cosets of  $N$  in  $G$  is a group with operation  $(aN)(bN) = abN$ .*

*Proof.* The verification of the definition of a group is very straightforward:

(1)  $N = eN$  is the identity:  $(eN)(aN) = eaN = aN$  and  $(aN)(eN) = aeN = aN$ .

(2) Multiplication of cosets is associative:

$$[(aN)(bN)](cN) = (abN)(cN) = abcN = (aN)(bcN) = (aN)[(bN)(cN)]$$

(3) The inverse of  $aN$  is  $a^{-1}N$ :

$$(aN)(a^{-1}N) = aa^{-1}N = eN$$

Therefore  $G/N$  is a group. □

**Theorem 14.2.** *If  $N$  is a normal subgroup of  $G$  then the mapping*

$$\gamma : G \rightarrow G/N$$

*given by  $\gamma(g) = gN$  is a surjective homomorphism.*

*Proof.* This is obvious from the definition. □

14.1. **Example:**  $\mathbb{Z}/n$ . Take the additive group  $G = \mathbb{Z}$ . Since this is abelian, all subgroups are normal. Take the subgroup  $4\mathbb{Z}$ . There are 4 cosets:

$$\mathbb{Z}, 1 + \mathbb{Z}, 2 + \mathbb{Z}, 3 + \mathbb{Z}$$

If we use the notation

$$\bar{x} := x + 4\mathbb{Z}$$

then the 4 cosets:  $\bar{0}, \bar{1}, \bar{2}, \bar{3}$  and  $\bar{0} = \bar{4} = \bar{8} = \bar{12} = \dots$  and similarly, the other cosets have many names. Addition is given by:

$$\bar{x} + \bar{y} = \overline{x + y}$$

This is just addition modulo 4. So,

$$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$$

The group  $\mathbb{Z}/n\mathbb{Z}$  is often just written  $\mathbb{Z}/n$ .

#### 14.2. Isomorphism theorems.

**Theorem 14.3.** *If  $\phi : G \rightarrow H$  is a homomorphism of groups with kernel  $K$  then the factor group  $G/K$  is isomorphic to the image of  $\phi$  and the isomorphism  $\bar{\phi} : G/K \rightarrow \text{im } \phi$  is given by*

$$\bar{\phi}(gK) = \phi(g)$$

*Proof.* (1) This is well defined (independent of the choice of  $g$ ) since  $gK = hK$  iff  $h^{-1}g \in K$  which implies that

$$\phi(h^{-1}g) = e = \phi(h)^{-1}\phi(g)$$

So,  $\phi(h) = \phi(g)$ .

(2)  $\bar{\phi}$  is clearly onto. (Why?)

(3) To show that  $\bar{\phi}$  is 1-1 suppose that  $\bar{\phi}(gK) = \bar{\phi}(hK)$ . Then  $\phi(g) = \phi(h)$  So,

$$\phi(g^{-1}h) = \phi(g)^{-1}\phi(h) = e$$

In other words,  $g^{-1}h \in K$ . But this is the same as saying that  $gK = hK$ . So,  $\bar{\phi}$  is 1-1.

(4) The homomorphism property:

$$\bar{\phi}(gKhK) = \bar{\phi}(ghK) = \phi(gh) = \phi(g)\phi(h) = \bar{\phi}(gK)\bar{\phi}(hK)$$

□

The original homomorphism  $\phi : G \rightarrow H$  is factored as a composition of three homomorphisms:

$$\phi = \iota \circ \bar{\phi} \circ \gamma : G \xrightarrow{\gamma} G/N \xrightarrow{\bar{\phi}} \text{im } \phi \xrightarrow{\iota} H$$

Problem: If  $N \triangleleft G$  what is the order of  $gN$  as an element in the group  $G/N$ ? How is the order of  $gN$  related to the order of  $g$ ? Take as an example  $G = \mathbb{Z}_{12}$ ,  $N = \langle 4 \rangle$ ,  $g = 2$ .

Answer: The order of  $gN$  is equal to the smallest positive integer  $k$  so that  $g^k \in N$ . In the example  $g = 2$ ,  $k = 2$  since  $2 + 2 = 4 \in N$ . This is related to the order of  $g$ :  $o(g) = n$  by the fact that  $k$  divides  $n$ . In the example,  $n = 6$  since  $6 \cdot 2 = 0$ .<sup>5</sup>

---

<sup>5</sup>The additive group notation is  $kg = g + g + \cdots + g$  instead of  $g^k = gg \cdots g$ . An additive group often has other operations defined and we want to make sure we are talking about the group operation which is addition and not the other operations which are usually not a group operations.