

subgroup is contained in one of these three. Draw the lattice of all subgroups of  $A$ , giving each subgroup in terms of at most two generators.

13. The group  $G = Z_2 \times Z_8 = \langle x, y \mid x^2 = y^8 = 1, xy = yx \rangle$  has order 16 and has three subgroups of order 8:  $\langle x, y^2 \rangle \cong Z_2 \times Z_4$ ,  $\langle y \rangle \cong Z_8$  and  $\langle xy \rangle \cong Z_8$  and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of  $G$ , giving each subgroup in terms of at most two generators (cf. Exercise 12).
14. Let  $M$  be the group of order 16 with the following presentation:

$$\langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$$

(sometimes called the *modular* group of order 16). It has three subgroups of order 8:  $\langle u, v^2 \rangle$ ,  $\langle v \rangle$  and  $\langle uv \rangle$  and every proper subgroup is contained in one of these three. Prove that  $\langle u, v^2 \rangle \cong Z_2 \times Z_4$ ,  $\langle v \rangle \cong Z_8$  and  $\langle uv \rangle \cong Z_8$ . Show that the lattice of subgroups of  $M$  is the same as the lattice of subgroups of  $Z_2 \times Z_8$  (cf. Exercise 13) but that these two groups are not isomorphic.

15. Describe the isomorphism type of each of the three subgroups of  $D_{16}$  of order 8.
16. Use the lattice of subgroups of the quasidihedral group of order 16 to show that every element of order 2 is contained in the proper subgroup  $\langle \tau, \sigma^2 \rangle$  (cf. Exercise 11).
17. Use the lattice of subgroups of the modular group  $M$  of order 16 to show that the set  $\{x \in M \mid x^2 = 1\}$  is a subgroup of  $M$  isomorphic to the Klein 4-group (cf. Exercise 14).
18. Use the lattice to help find the centralizer of every element of  $QD_{16}$  (cf. Exercise 11).
19. Use the lattice to help find  $N_{D_{16}}(\langle s, r^4 \rangle)$ .
20. Use the lattice of subgroups of  $QD_{16}$  (cf. Exercise 11) to help find the normalizers
- (a)  $N_{QD_{16}}(\langle \tau\sigma \rangle)$       (b)  $N_{QD_{16}}(\langle \tau, \sigma^4 \rangle)$ .

## Quotient Groups and Homomorphisms

### 3.1 DEFINITIONS AND EXAMPLES

In this chapter we introduce the notion of a *quotient* group of a group  $G$ , which is another way of obtaining a “smaller” group from the group  $G$  and, as we did with subgroups, we shall use quotient groups to study the structure of  $G$ . The structure of the group  $G$  is reflected in the structure of the quotient groups and the subgroups of  $G$ . For example, we shall see that the lattice of subgroups for a *quotient* of  $G$  is reflected at the “top” (in a precise sense) of the lattice for  $G$  whereas the lattice for a *subgroup* of  $G$  occurs naturally at the “bottom.” One can therefore obtain information about the group  $G$  by combining this information and we shall indicate how some classification theorems arise in this way.

The study of the quotient groups of  $G$  is essentially equivalent to the study of the homomorphisms of  $G$ , i.e., the maps of the group  $G$  to another group which respect the group structures. If  $\varphi$  is a homomorphism from  $G$  to a group  $H$  recall that the *fibers* of  $\varphi$  are the sets of elements of  $G$  projecting to single elements of  $H$ , which we can represent pictorially in Figure 1, where the vertical line in the box above a point  $a$  represents the fiber of  $\varphi$  over  $a$ .

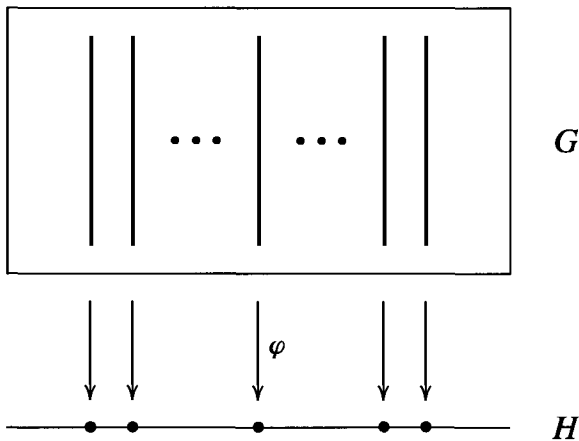


Fig. 1

The group operation in  $H$  provides a way to multiply two elements in the image of  $\varphi$  (i.e., two elements on the horizontal line in Figure 1). This suggests a natural multiplication of the *fibers* lying above these two points making *the set of fibers into a group*: if  $X_a$  is the fiber above  $a$  and  $X_b$  is the fiber above  $b$  then the product of  $X_a$  with  $X_b$  is defined to be the fiber  $X_{ab}$  above the product  $ab$ , i.e.,  $X_a X_b = X_{ab}$ . This multiplication is associative since multiplication is associative in  $H$ , the identity is the fiber over the identity of  $H$ , and the inverse of the fiber over  $a$  is the fiber over  $a^{-1}$ , as is easily checked from the definition. For example, the associativity is proved as follows:  $(X_a X_b) X_c = (X_{ab}) X_c = X_{(ab)c}$  and  $X_a (X_b X_c) = X_a (X_{bc}) = X_{a(bc)}$ . Since  $(ab)c = a(bc)$  in  $H$ ,  $(X_a X_b) X_c = X_a (X_b X_c)$ . Roughly speaking, the group  $G$  is partitioned into pieces (the fibers) and these pieces themselves have the structure of a group, called a *quotient* group of  $G$  (a formal definition follows the example below).

Since the multiplication of fibers is defined from the multiplication in  $H$ , by construction the quotient group with this multiplication is naturally isomorphic to the image of  $G$  under the homomorphism  $\varphi$  (fiber  $X_a$  is identified with its image  $a$  in  $H$ ).

### Example

Let  $G = \mathbb{Z}$ , let  $H = Z_n = \langle x \rangle$  be the cyclic group of order  $n$  and define  $\varphi : \mathbb{Z} \rightarrow Z_n$  by  $\varphi(a) = x^a$ . Since

$$\varphi(a + b) = x^{a+b} = x^a x^b = \varphi(a) \varphi(b)$$

it follows that  $\varphi$  is a homomorphism (note that the operation in  $\mathbb{Z}$  is addition and the operation in  $Z_n$  is multiplication). Note also that  $\varphi$  is surjective. The fiber of  $\varphi$  over  $x^a$  is then

$$\begin{aligned} \varphi^{-1}(x^a) &= \{m \in \mathbb{Z} \mid x^m = x^a\} = \{m \in \mathbb{Z} \mid x^{m-a} = 1\} \\ &= \{m \in \mathbb{Z} \mid n \text{ divides } m - a\} \quad (\text{by Proposition 2.3}) \\ &= \{m \in \mathbb{Z} \mid m \equiv a \pmod{n}\} = \bar{a}, \end{aligned}$$

i.e., the fibers of  $\varphi$  are precisely the residue classes modulo  $n$ . Figure 1 here becomes:

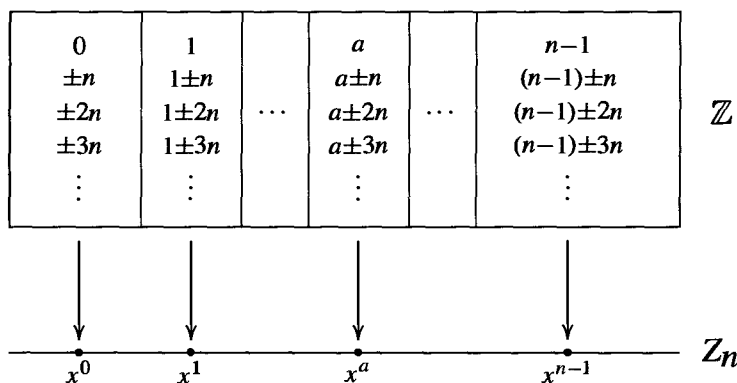


Fig. 2

The multiplication in  $Z_n$  is just  $x^a x^b = x^{a+b}$ . The corresponding fibers are  $\bar{a}$ ,  $\bar{b}$ , and  $\overline{a+b}$ , so the corresponding group operation for the fibers is  $\bar{a} \cdot \bar{b} = \overline{a+b}$ . This is just the group  $\mathbb{Z}/n\mathbb{Z}$  under addition, a group isomorphic to the image of  $\varphi$  (all of  $Z_n$ ).

The identity of this group (the fiber above the identity in  $Z_n$ ) consists of all the multiples of  $n$  in  $\mathbb{Z}$ , namely  $n\mathbb{Z}$ , a *subgroup* of  $\mathbb{Z}$ , and the remaining fibers are just translates,  $a + n\mathbb{Z}$ , of this subgroup. The group operation can also be defined directly by taking *representatives* from these fibers, adding these representatives in  $\mathbb{Z}$  and taking the fiber containing this sum (this was the original definition of the group  $\mathbb{Z}/n\mathbb{Z}$ ). From a computational point of view computing the product of  $\bar{a}$  and  $\bar{b}$  by simply adding representatives  $a$  and  $b$  is much easier than first computing the image of these fibers under  $\varphi$  (namely,  $x^a$  and  $x^b$ ), multiplying these in  $H$  (obtaining  $x^{a+b}$ ) and then taking the fiber over this product.

We first consider some basic properties of homomorphisms and their fibers. The fiber of a homomorphism  $\varphi : G \rightarrow H$  lying above the identity of  $H$  is given a name:

**Definition.** If  $\varphi$  is a homomorphism  $\varphi : G \rightarrow H$ , the *kernel* of  $\varphi$  is the set

$$\{g \in G \mid \varphi(g) = 1\}$$

and will be denoted by  $\ker \varphi$  (here 1 is the identity of  $H$ ).

**Proposition 1.** Let  $G$  and  $H$  be groups and let  $\varphi : G \rightarrow H$  be a homomorphism.

- (1)  $\varphi(1_G) = 1_H$ , where  $1_G$  and  $1_H$  are the identities of  $G$  and  $H$ , respectively.
- (2)  $\varphi(g^{-1}) = \varphi(g)^{-1}$  for all  $g \in G$ .
- (3)  $\varphi(g^n) = \varphi(g)^n$  for all  $n \in \mathbb{Z}$ .
- (4)  $\ker \varphi$  is a subgroup of  $G$ .
- (5)  $\text{im}(\varphi)$ , the image of  $G$  under  $\varphi$ , is a subgroup of  $H$ .

*Proof:* (1) Since  $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$ , the cancellation laws show that (1) holds.

(2)  $\varphi(1_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$  and, by part (1),  $\varphi(1_G) = 1_H$ , hence

$$1_H = \varphi(g)\varphi(g^{-1}).$$

Multiplying both sides on the left by  $\varphi(g)^{-1}$  and simplifying gives (2).

(3) This is an easy exercise in induction for  $n \in \mathbb{Z}^+$ . By part (2), conclusion (3) holds for negative values of  $n$  as well.

(4) Since  $1_G \in \ker \varphi$ , the kernel of  $\varphi$  is not empty. Let  $x, y \in \ker \varphi$ , that is  $\varphi(x) = \varphi(y) = 1_H$ . Then

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = 1_H 1_H^{-1} = 1_H$$

that is,  $xy^{-1} \in \ker \varphi$ . By the subgroup criterion,  $\ker \varphi \leq G$ .

(5) Since  $\varphi(1_G) = 1_H$ , the identity of  $H$  lies in the image of  $\varphi$ , so  $\text{im}(\varphi)$  is nonempty. If  $x$  and  $y$  are in  $\text{im}(\varphi)$ , say  $x = \varphi(a)$ ,  $y = \varphi(b)$ , then  $y^{-1} = \varphi(b^{-1})$  by (2) so that  $xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$  since  $\varphi$  is a homomorphism. Hence also  $xy^{-1}$  is in the image of  $\varphi$ , so  $\text{im}(\varphi)$  is a subgroup of  $H$  by the subgroup criterion.

We can now define some terminology associated with quotient groups.

**Definition.** Let  $\varphi : G \rightarrow H$  be a homomorphism with kernel  $K$ . The *quotient group* or *factor group*,  $G/K$  (read  $G$  modulo  $K$  or simply  $G \bmod K$ ), is the group whose elements are the fibers of  $\varphi$  with group operation defined above: namely if  $X$  is the fiber above  $a$  and  $Y$  is the fiber above  $b$  then the product of  $X$  with  $Y$  is defined to be the fiber above the product  $ab$ .

The notation emphasizes the fact that the kernel  $K$  is a *single element* in the group  $G/K$  and we shall see below (Proposition 2) that, as in the case of  $\mathbb{Z}/n\mathbb{Z}$  above, the other elements of  $G/K$  are just the “translates” of the kernel  $K$ . Hence we may think of  $G/K$  as being obtained by collapsing or “dividing out” by  $K$  (or more precisely, by equivalence modulo  $K$ ). This explains why  $G/K$  is referred to as a “quotient” group.

The definition of the quotient group  $G/K$  above requires the map  $\varphi$  explicitly, since the multiplication of the fibers is performed by first projecting the fibers to  $H$  via  $\varphi$ , multiplying in  $H$  and then determining the fiber over this product. Just as for  $\mathbb{Z}/n\mathbb{Z}$  above, it is also possible to define the multiplication of fibers directly in terms of *representatives* from the fibers. This is computationally simpler and the map  $\varphi$  does not enter explicitly. We first show that the fibers of a homomorphism can be expressed in terms of the kernel of the homomorphism just as in the example above (where the kernel was  $n\mathbb{Z}$  and the fibers were translates of the form  $a + n\mathbb{Z}$ ).

**Proposition 2.** Let  $\varphi : G \rightarrow H$  be a homomorphism of groups with kernel  $K$ . Let  $X \in G/K$  be the fiber above  $a$ , i.e.,  $X = \varphi^{-1}(a)$ . Then

- (1) For any  $u \in X$ ,  $X = \{uk \mid k \in K\}$
- (2) For any  $u \in X$ ,  $X = \{ku \mid k \in K\}$ .

*Proof:* We prove (1) and leave the proof of (2) as an exercise. Let  $u \in X$  so, by definition of  $X$ ,  $\varphi(u) = a$ . Let

$$uK = \{uk \mid k \in K\}.$$

We first prove  $uK \subseteq X$ . For any  $k \in K$ ,

$$\begin{aligned} \varphi(uk) &= \varphi(u)\varphi(k) && \text{(since } \varphi \text{ is a homomorphism)} \\ &= \varphi(u)1 && \text{(since } k \in \ker \varphi) \\ &= a, \end{aligned}$$

that is,  $uk \in X$ . This proves  $uK \subseteq X$ . To establish the reverse inclusion suppose  $g \in X$  and let  $k = u^{-1}g$ . Then

$$\begin{aligned} \varphi(k) &= \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) && \text{(by Proposition 1)} \\ &= a^{-1}a = 1. \end{aligned}$$

Thus  $k \in \ker \varphi$ . Since  $k = u^{-1}g$ ,  $g = uk \in uK$ , establishing the inclusion  $X \subseteq uK$ . This proves (1).

The sets arising in Proposition 2 to describe the fibers of a homomorphism  $\varphi$  are defined for *any* subgroup  $K$  of  $G$ , not necessarily the kernel of some homomorphism (we shall determine necessary and sufficient conditions for a subgroup to be such a kernel shortly) and are given a name: