

# Dummit & Foote Ch. 3.1: Quotient Groups and Homomorphisms

Scott Donaldson

Aug. - Sep. 2023

Let  $G$  and  $H$  be groups.

## 1. (8/21/23)

Let  $\varphi : G \rightarrow H$  be a homomorphism and let  $E \leq H$ . Prove that  $\varphi^{-1}(E) \leq G$  (i.e., the preimage or pullback of a subgroup under a homomorphism is a subgroup). If  $E \trianglelefteq H$  prove that  $\varphi^{-1}(E) \trianglelefteq G$ . Deduce that  $\ker \varphi \trianglelefteq G$ .

*Proof.* Let  $x, y \in \varphi^{-1}(E) \subseteq G$ . Suppose that  $\varphi(x) = a, \varphi(y) = b, a, b \in E \leq H$ . Since  $\varphi$  is a homomorphism, we have  $\varphi(y^{-1}) = \varphi(y)^{-1} = b^{-1}$ . Then:

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = ab^{-1} \in E,$$

which implies that  $xy^{-1} \in \varphi^{-1}(E)$ . It follows that, by the subgroup criterion,  $\varphi^{-1}(E) \leq G$ .  $\square$

## 2. (8/23/23)

Let  $\varphi : G \rightarrow H$  be a homomorphism of groups with kernel  $K$  and let  $a, b \in \varphi(G)$ . Let  $X \in G/K$  be the fiber above  $a$  and  $Y$  be the fiber above  $b$ , i.e.,  $X = \varphi^{-1}(a), Y = \varphi^{-1}(b)$ . Fix an element  $x \in X$  (so  $\varphi(x) = a$ ). Prove that if  $XY = Z$  in the quotient group  $G/K$  and  $z$  is any member of  $Z$ , then there is some  $y \in Y$  such that  $xy = z$ .

*Proof.* We know that, for any  $x \in X, y \in Y$ ,  $\varphi(x) = a$  and  $\varphi(y) = b$ . Since  $\varphi$  is a homomorphism, it follows that  $\varphi(xy) = \varphi(x)\varphi(y) = ab$ , and so the image of any element of  $XY = Z$  under  $\varphi$  is  $ab \in H$ .

Next, consider the element  $x^{-1}z \in G$ , as well as its image under  $\varphi$ . Since  $\varphi$  is a homomorphism, we have  $\varphi(x^{-1}) = \varphi(x)^{-1}$ . So  $\varphi(x^{-1}z) = \varphi(x^{-1})\varphi(z) = \varphi(x)^{-1}\varphi(z) = a^{-1}ab = b$ . The set  $Y$  consists of all elements of  $G$  whose image under  $\varphi$  is  $b$ , and so we must have  $x^{-1}z \in Y$ .

Now if we fix some element  $x \in X$ , then for any  $z \in Z$ , we have  $x^{-1}z \in Y$  such that its product with  $x$  is  $z$ :  $xx^{-1}z = z$ .  $\square$

### 3. (8/23/23)

Let  $A$  be an abelian group and let  $B$  be a subgroup of  $A$ . Prove that  $A/B$  is abelian. Give an example of a non-abelian group  $G$  containing a proper normal subgroup  $N$  such that  $G/N$  is abelian.

*Proof.* Because  $A$  is abelian, all subgroups of  $A$  are normal, so  $A/B$  is well-defined for every  $B \leq A$ .

Let  $C, D \in A/B$  with  $C = cB$  and  $D = dB$  for some  $c, d \in A$ . Then:

$$CD = (cB)(dB) = (cd)B = (dc)B = (dB)(cB) = DC,$$

which implies that  $A/B$  is abelian.

Now if we let  $G$  be the dihedral group  $D_8$ , then  $G$  is non-abelian. Let  $N$  be the cyclic subgroup generated by  $r : \{1, r, r^2, r^3\}$ . The only coset of  $N$  is  $sN$ ; together these two sets cover  $G$ . Then  $G/N = \{N, sN\}$ . There is only one group of order 2 up to isomorphism, and it is abelian. Thus  $G/N$  is abelian.  $\square$

### 4. (8/23/23)

Prove that in the quotient group  $G/N$ ,  $(gN)^\alpha = (g^\alpha)N$  for all  $\alpha \in \mathbb{Z}$ .

*Proof.* We start by induction: In the base case,  $\alpha = 1$ , we have  $(gN)^1 = gN = (g^1)N$ . Next, suppose that for some  $\alpha > 1$ , we have  $(gN)^\alpha = (g^\alpha)N$ . Then:

$$(gN)^{\alpha+1} = (gN)^\alpha gN = g^\alpha N \cdot gN = (g^{\alpha+1})N,$$

as desired. We have now proven that  $(gN)^\alpha = (g^\alpha)N$  for  $\alpha \geq 1$ .

Next, consider  $(gN)^\alpha (gN)^{-\alpha}$ , where  $\alpha \geq 1$ . In the quotient group  $G/N$ , for any subset  $X \in G/N$ , we must have  $X^\alpha X^{-\alpha} = N$  (the identity of  $G/N$ ), so  $(gN)^\alpha (gN)^{-\alpha} = N$ . From above,  $(gN)^\alpha = (g^\alpha)N$ , so  $(g^\alpha)N \cdot (gN)^{-\alpha} = N$ . Also, from the operation on left cosets, we know that  $N = (g^\alpha)N \cdot (g^{-\alpha})N$ . Since both  $(g^\alpha)N \cdot (gN)^{-\alpha} = N$  and  $(g^\alpha)N \cdot (g^{-\alpha})N = N$ , we must have  $(gN)^{-\alpha} = (g^{-\alpha})N$ . We have now proven for all nonzero integers.

Finally, we note that  $(gN)^0 = N$  (the identity of  $G/N$ ) and that  $(g^0)N = eN = N$ , so  $(gN)^0 = (g^0)N$ . This concludes the proof that  $(gN)^\alpha = (g^\alpha)N$  for all  $\alpha \in \mathbb{Z}$ .  $\square$

### 5. (8/23/23)

Use the preceding exercise to prove that the order of the element  $gN$  in  $G/N$  is  $n$ , where  $n$  is the smallest positive integer such that  $g^n \in N$  (and  $gN$  has infinite order if no such positive integer exists). Give an example to show that the order of  $gN$  in  $G/N$  may be strictly smaller than the order of  $g$  in  $G$ .

*Proof.* Let  $gN \in G/N$ , and let  $n$  be the smallest positive integer such that  $g^n \in N$ . Suppose that  $g^n = h \in N$ .

From Exercise 4.,  $(gN)^n = (g^n)N = hN = N$  (because  $h \in N$ ), so the order of  $gN$  must divide  $n$ .

Suppose (toward contradiction) that the order of  $gN$  is  $k$ , where  $k < n$ . Then  $(gN)^k = (g^k)N = N$ , which implies that  $g^k$  lies in  $N$ , contradicting our assumption that  $n$  is the smallest such positive integer. Therefore the order of  $gN$  is  $n$ .

If there is no positive integer  $n$  such that  $g^n \in N$ , then for all  $k \in \mathbb{Z}^+$ , we have  $(gN)^k = (g^k)N \neq N$ , so  $gN$  has infinite order.

As an example where  $|gN| < |g|$ , let  $G = Z_9 = \langle x \rangle$  and let  $N = \langle x^3 \rangle$ . Because all cyclic groups are abelian,  $N$  is normal in  $G$ , and so  $G/N$  is well-defined. The quotient group  $G/N$  contains three elements:  $N, xN$ , and  $(x^2)N$ . The element  $xN \in G/N$  has order 3:  $(xN)^3 = (x^3)N = N$  (because  $x^3 \in N$ ). However, the generating element  $x \in G$  has order 9.  $\square$

## 6. (8/24/23)

Define  $\varphi : \mathbb{R}^\times \rightarrow \{\pm 1\}$  by letting  $\varphi(x)$  be  $x$  divided by the absolute value of  $x$ . Describe the fibers of  $\varphi$  and prove that  $\varphi$  is a homomorphism.

*Proof.* We consider the two cases where  $x < 0$  and  $x > 0$  ( $0$  is not an element of  $\mathbb{R}^\times$ ). If  $x > 0$ , then  $\varphi(x) = x/|x| = x/x = 1$ . If  $x < 0$ , then  $\varphi(x) = x/|x| = x/-x = -1$ . Therefore the fiber above  $-1$  is every negative real number and the fiber above  $1$  is every positive real number.

To show that  $\varphi$  is a homomorphism, we let  $x, y \in \mathbb{R}^\times$  and again consider the different cases: Where  $x$  and  $y$  are both positive, where they are both negative, and where one is positive and the other negative.

If both  $x$  and  $y$  are positive, then  $\varphi(x)\varphi(y) = 1 \cdot 1 = 1$  and  $\varphi(xy) = \frac{xy}{|xy|} = \frac{xy}{xy} = 1$ , so  $\varphi(x)\varphi(y) = \varphi(xy)$ .

If both  $x$  and  $y$  are negative, then  $\varphi(x)\varphi(y) = -1 \cdot -1 = 1$  and  $\varphi(xy) = \frac{xy}{|xy|} = \frac{xy}{xy} = 1$ , so  $\varphi(x)\varphi(y) = \varphi(xy)$ .

Suppose  $x$  is positive and  $y$  is negative. Then  $\varphi(x)\varphi(y) = 1 \cdot -1 = -1$  and  $\varphi(xy) = \frac{xy}{|xy|} = \frac{xy}{-xy} = -1$ , so  $\varphi(x)\varphi(y) = \varphi(xy)$ .

Thus, in every case of  $x, y \in \mathbb{R}^\times$ , we have  $\varphi(x)\varphi(y) = \varphi(xy)$ , and  $\varphi$  is thus a homomorphism.  $\square$

## 7. (8/24/23)

Define  $\pi : \mathbb{R}^2 \rightarrow \mathbb{R}$  by  $\pi((x, y)) = x + y$ . Prove that  $\pi$  is a surjective homomorphism and describe the kernel and fibers of  $\pi$  geometrically.

*Proof.* First, to show that  $\pi$  is surjective, let  $z \in \mathbb{R}$ . Now  $z = z + 0$ , so  $(z, 0)$  is an element of  $\mathbb{R}^2$  such that  $\pi((z, 0)) = z + 0 = z$ .

Next, to show that  $\pi$  is a homomorphism, let  $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ . We have  $\pi((x_1, y_1) + (x_2, y_2)) = \pi((x_1 + x_2, y_1 + y_2)) = x_1 + x_2 + y_1 + y_2$ , and  $\pi((x_1, y_1)) + \pi((x_2, y_2)) = x_1 + y_1 + x_2 + y_2$ . By the commutativity of addition in  $\mathbb{R}$ , these are equal to each other, and so  $\pi$  is a surjective homomorphism.

The kernel of  $\pi$  consists of all points  $(x, y) \in \mathbb{R}^2$  such that  $x + y = 0$ , that is, the diagonal line running from the upper-left to the bottom-right of the Cartesian plane. Geometrically, the fibers of  $\pi$  are translations of this line, such that for any  $z \in \mathbb{R}$ , the fiber of  $\pi$  above  $z$  is the diagonal line intersecting both  $(z, 0)$  and  $(0, z)$ .  $\square$

## 8. (8/24/23)

Let  $\varphi : \mathbb{R}^\times \rightarrow \mathbb{R}^\times$  be the map sending  $x$  to the absolute value of  $x$ . Prove that  $\varphi$  is a homomorphism and find the image of  $\varphi$ . Describe the kernel and the fibers of  $\varphi$ .

*Proof.* Let  $x, y \in \mathbb{R}^\times$  (so  $x \neq 0, y \neq 0$ ). If both  $x$  and  $y$  are positive or both are negative, then:

$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y),$$

and if  $x$  is positive and  $y$  is negative, then:

$$\varphi(xy) = |xy| = x(-y) = |x||y| = \varphi(x)\varphi(y),$$

so  $\varphi$  is a homomorphism.

The image of  $\varphi$  consists of every positive real number. The kernel of  $\varphi$  is the set  $\{x \in \mathbb{R}^\times \mid |x| = 1\}$ , that is,  $\{\pm 1\}$ . For a given element  $z > 0$ , the fiber of  $\varphi$  above  $z$  is the set  $\{\pm z\}$ .  $\square$

## 9. (8/25/23)

Define  $\varphi : \mathbb{C}^\times \rightarrow \mathbb{R}^\times$  by  $\varphi(a + bi) = a^2 + b^2$ . Prove that  $\varphi$  is a homomorphism and find the image of  $\varphi$ . Describe the kernel and the fibers of  $\varphi$  geometrically (as subsets of the plane).

*Proof.* To show that  $\varphi$  is a homomorphism, let  $z_1 = a_1 + b_1i, z_2 = a_2 + b_2i \in \mathbb{C}^\times$ . We calculate:

$$\begin{aligned} \varphi(z_1 z_2) &= \varphi((a_1 + b_1i)(a_2 + b_2i)) \\ &= \varphi((a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i) \\ &= (a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + a_2 b_1)^2 \\ &= a_1^2 a_2^2 - 2a_1 a_2 b_1 b_2 + b_1^2 b_2^2 + a_1^2 b_2^2 + 2a_1 a_2 b_1 b_2 + a_2^2 b_1^2 \\ &= a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2, \text{ and} \\ \varphi(z_1)\varphi(z_2) &= \varphi(a_1 + b_1i)\varphi(a_2 + b_2i) = (a_1^2 + b_1^2)(a_2^2 + b_2^2) \\ &= a_1^2 a_2^2 + b_1^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2, \end{aligned}$$

which proves that  $\varphi$  is a homomorphism.

The image of a complex number  $a + bi$  under  $\varphi$  is  $a^2 + b^2$ , which is always non-negative because it is the sum of two non-negative numbers. Since both  $\mathbb{C}^\times$  and  $\mathbb{R}^\times$  exclude 0, the image of  $\varphi$  is therefore all positive real numbers.

The kernel of  $\varphi$  are those complex numbers whose image under  $\varphi$  is 1. Geometrically,  $\varphi$  is a map from a point in the complex plane to its length, or distance from zero. Therefore the kernel of  $\varphi$  is the unit circle in the complex plane. The fibers of a given positive real number  $x$  is the circle of radius  $x$  centered at the origin in the complex plane.  $\square$