PEARSON NEW INTERNATIONAL EDITION

A First Course in Abstract Algebra

John B. Fraleigh

Seventh Edition

ALWAYS LEARNING

PEARSON

Pearson New International Edition

A First Course in Abstract Algebra
John B. Fraleigh
Seventh Edition

PEARSON

19. Ker(ϕ) and $\phi(20)$ for $\phi : \mathbb{Z} \to S_8$ such that $\phi(1) = (1, 4, 2, 6)(2, 5, 7)$

20. Ker(ϕ) and $\phi(3)$ for $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$ such that $\phi(1) = 8$

21. Ker(ϕ) and $\phi(14)$ for $\phi : \mathbb{Z}_{24} \to S_8$ where $\phi(1) = (2, 5)(1, 4, 6, 7)$

22. Ker(ϕ) and $\phi(-3, 2)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi(1, 0) = 3$ and $\phi(0, 1) = -5$

23. Ker(ϕ) and $\phi(4, 6)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $\phi(1, 0) = (2, -3)$ and $\phi(0, 1) = (-1, 5)$

24. Ker(ϕ) and $\phi(3, 10)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to S_{10}$ where $\phi(1, 0) = (3, 5)(2, 4)$ and $\phi(0, 1) = (1, 7)(6, 10, 8, 9)$

25. How many homomorphisms are there of $\mathbb{Z}$ onto $\mathbb{Z}$?

26. How many homomorphisms are there of $\mathbb{Z}$ into $\mathbb{Z}$?

27. How many homomorphisms are there of $\mathbb{Z}$ into $\mathbb{Z}_2$?

28. Let G be a group, and let $g \in G$. Let $\phi_g : G \to G$ be defined by $\phi_g(x) = gx$ for $x \in G$. For which $g \in G$ is ϕ_g a homomorphism?

29. Let G be a group, and let $g \in G$. Let $\phi_g : G \to G$ be defined by $\phi_g(x) = gxg^{-1}$ for $x \in G$. For which $g \in G$ is ϕ_g a homomorphism?

Concepts

In Exercises 30 and 31, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

30. A *homomorphism* is a map such that $\phi(xy) = \phi(x)\phi(y)$.

31. Let $\phi : G \to G'$ be a homomorphism of groups. The *kernel of* ϕ is $\{x \in G \mid \phi(x) = e'\}$ where e' is the identity in G'.

32. Mark each of the following true or false.

_______ **a.** A_n is a normal subgroup of S_n.

_______ **b.** For any two groups G and G', there exists a homomorphism of G into G'.

_______ **c.** Every homomorphism is a one-to-one map.

_______ **d.** A homomorphism is one to one if and only if the kernel consists of the identity element alone.

_______ **e.** The image of a group of 6 elements under some homomorphism may have 4 elements. (See Exercise 44.)

_______ **f.** The image of a group of 6 elements under a homomorphism may have 12 elements.

_______ **g.** There is a homomorphism of some group of 6 elements into some group of 12 elements.

_______ **h.** There is a homomorphism of some group of 6 elements into some group of 10 elements.

_______ **i.** A homomorphism may have an empty kernel.

_______ **j.** It is not possible to have a nontrivial homomorphism of some finite group into some infinite group.

In Exercises 33 through 43, give an example of a nontrivial homomorphism ϕ for the given groups, if an example exists. If no such homomorphism exists, explain why that is so. You may use Exercises 44 and 45.

33. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_5$

34. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4$

35. $\phi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_5$

36. $\phi : \mathbb{Z}_3 \to \mathbb{Z}$

37. $\phi : \mathbb{Z}_3 \to S_3$

38. $\phi : \mathbb{Z} \to S_3$

39. $\phi : \mathbb{Z} \times \mathbb{Z} \to 2\mathbb{Z}$

40. $\phi : 2\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$

41. $\phi : D_4 \to S_3$

42. $\phi : S_3 \to S_4$

43. $\phi : S_4 \to S_3$

Theory

44. Let $\phi : G \to G'$ be a group homomorphism. Show that if $|G|$ is finite, then $|\phi[G]|$ is finite and is a divisor of $|G|$.

45. Let $\phi : G \to G'$ be a group homomorphism. Show that if $|G'|$ is finite, then, $|\phi[G]|$ is finite and is a divisor of $|G'|$.

46. Let a group G be generated by $\{a_i \mid i \in I\}$, where I is some indexing set and $a_i \in G$ for all $i \in I$. Let $\phi : G \to G'$ and $\mu : G \to G'$ be two homomorphisms from G into a group G', such that $\phi(a_i) = \mu(a_i)$ for every $i \in I$. Prove that $\phi = \mu$. [Thus, for example, a homomorphism of a cyclic group is completely determined by its value on a generator of the group.] [*Hint*: Use Theorem 7.6 and, of course, Definition 13.1.]

47. Show that any group homomorphism $\phi : G \to G'$ where $|G|$ is a prime must either be the trivial homomorphism or a one-to-one map.

48. The **sign of an even permutation** is $+1$ and the **sign of an odd permutation** is -1. Observe that the map $\mathrm{sgn}_n : S_n \to \{1, -1\}$ defined by

$$\mathrm{sgn}_n(\sigma) = \text{sign of } \sigma$$

is a homomorphism of S_n onto the multiplicative group $\{1, -1\}$. What is the kernel? Compare with Example 13.3.

49. Show that if G, G', and G'' are groups and if $\phi : G \to G'$ and $\gamma : G' \to G''$ are homomorphisms, then the composite map $\gamma\phi : G \to G''$ is a homomorphism.

50. Let $\phi : G \to H$ be a group homomorphism. Show that $\phi[G]$ is abelian if and only if for all $x, y \in G$, we have $xyx^{-1}y^{-1} \in \mathrm{Ker}(\phi)$.

51. Let G be any group and let a be any element of G. Let $\phi : \mathbb{Z} \to G$ be defined by $\phi(n) = a^n$. Show that ϕ is a homomorphism. Describe the image and the possibilities for the kernel of ϕ.

52. Let $\phi : G \to G'$ be a homomorphism with kernel H and let $a \in G$. Prove the set equality $\{x \in G \mid \phi(x) = \phi(a)\} = Ha$.

53. Let G be a group, Let $h, k \in G$ and let $\phi : \mathbb{Z} \times \mathbb{Z} \to G$ be defined by $\phi(m, n) = h^m k^n$. Give a necessary and sufficient condition, involving h and k, for ϕ to be a homomorphism. Prove your condition.

54. Find a necessary and sufficient condition on G such that the map ϕ described in the preceding exercise is a homomorphism for *all* choices of $h, k \in G$.

55. Let G be a group, h an element of G, and n a positive integer. Let $\phi : \mathbb{Z}_n \to G$ be defined by $\phi(i) = h^i$ for $0 \le i \le n$. Give a necessary and sufficient condition (in terms of h and n) for ϕ to be a homomorphism. Prove your assertion.

SECTION 14 FACTOR GROUPS

Let H be a subgroup of a finite group G. Suppose we write a table for the group operation of G, listing element heads at the top and at the left as they occur in the left cosets of H. We illustrated this in Section 10. The body of the table may break up into blocks corresponding to the cosets (Table 10.5), giving a group operation on the cosets, or they may not break up that way (Table 10.9). We start this section by showing that if H is the kernel of a group homomorphism $\phi : G \to G'$, then the cosets of H (remember that left and right cosets then coincide) are indeed elements of a group whose binary operation is derived from the group operation of G.

Factor Groups from Homomorphisms

Let G be a group and let S be a set having the same cardinality as G. Then there is a one-to-one correspondence $\leftrightarrow$ between S and G. We can use $\leftrightarrow$ to define a binary operation on S, making S into a group isomorphic to G. Naively, we simply use the correspondence to rename each element of G by the name of its corresponding (under $\leftrightarrow$) element in S. We can describe explicitly the computation of xy for $x, y \in S$ as follows:

$$\text{if } x \leftrightarrow g_1 \quad \text{and} \quad y \leftrightarrow g_2 \quad \text{and} \quad z \leftrightarrow g_1g_2, \quad \text{then} \quad xy = z. \tag{1}$$

The direction $\rightarrow$ of the one-to-one correspondence $s \leftrightarrow g$ between $s \in S$ and $g \in G$ gives us a one-to-one function μ mapping S onto G. (Of course, the direction $\leftarrow$ of $\leftrightarrow$ gives us the inverse function μ^{-1}). Expressed in terms of μ, the computation (1) of xy for $x, y \in S$ becomes

$$\text{if } \mu(x) = g_1 \quad \text{and} \quad \mu(y) = g_2 \quad \text{and} \quad \mu(z) = g_1g_2, \quad \text{then} \quad xy = z. \tag{2}$$

The map $\mu : S \to G$ now becomes an isomorphism mapping the group S onto the group G. Notice that from (2), we obtain $\mu(xy) = \mu(z) = g_1g_2 = \mu(x)\mu(y)$, the required homomorphism property.

Let G and G' be groups, let $\phi : G \to G'$ be a homomorphism, and let $H = \mathrm{Ker}(\phi)$. Theorem 13.15 shows that for $a \in G$, we have $\phi^{-1}[\{\phi(a)\}] = aH = Ha$. We have a one-to-one correspondence $aH \leftrightarrow \phi(a)$ between cosets of H in G and elements of the subgroup $\phi[G]$ of G'. Remember that if $x \in aH$, so that $x = ah$ for some $h \in H$, then $\phi(x) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a)$, so the computation of the element of $\phi[G]$ corresponding to the coset $aH = xH$ is the same whether we compute it as $\phi(a)$ or as $\phi(x)$. Let us denote the set of all cosets of H by G/H. (We read G/H as "G over H" or as "G modulo H" or as "G mod H," but *never* as "G divided by H.")

In the preceding paragraph, we started with a homomorphism $\phi : G \to G'$ having kernel H, and we finished with the set G/H of cosets in one-to-one correspondence with the elements of the group $\phi[G]$. In our work above that, we had a set S with elements in one-to-one correspondence with those of a group G, and we made S into a group isomorphic to G with an isomorphism μ. Replacing S by G/H and replacing G by $\phi[G]$ in that construction, we can consider G/H to be a group isomorphic to $\phi[G]$ with that isomorphism μ. In terms of G/H and $\phi[G]$, the computation (2) of the product $(xH)(yH)$ for $xH, yH \in G/H$ becomes

$$\begin{aligned}&\text{if } \mu(xH) = \phi(x) \quad \text{and} \quad \mu(yH) = \phi(y) \quad \text{and} \quad \mu(zH) = \phi(x)\phi(y),\\ &\text{then} \quad (xH)(yH) = zH.\end{aligned} \tag{3}$$

But because ϕ is a homomorphism, we can easily find $z \in G$ such that $\mu(zH) = \phi(x)\phi(y)$; namely, we take $z = xy$ in G, and find that

$$\mu(zH) = \mu(xyH) = \phi(xy) = \phi(x)\phi(y).$$

This shows that the product $(xH)(yH)$ of two cosets is the coset $(xy)H$ that contains the product xy of x and y in G. While this computation of $(xH)(yH)$ may seem to depend on our choices x from xH and y from yH, our work above shows it does not. We demonstrate it again here because it is such an important point. If $h_1, h_2 \in H$ so that xh_1 is an element of xH and yh_2 is an element of yH, then there exists $h_3 \in H$ such that $h_1 y = yh_3$ because $Hy = yH$ by Theorem 13.15. Thus we have

$$(xh_1)(yh_2) = x(h_1 y)h_2 = x(yh_3)h_2 = (xy)(h_3 h_2) \in (xy)H,$$

so we obtain the same coset. Computation of the product of two cosets is accomplished by *choosing* an element from each coset and taking, as product of the cosets, the coset that contains the product in G of the choices. Any time we define something (like a product) in terms of choices, it is important to show that it is **well defined,** which means that it is independent of the choices made. This is precisely what we have just done. We summarize this work in a theorem.

14.1 Theorem Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a **factor group**, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.

14.2 Example Example 13.10 considered the map $\gamma : \mathbb{Z} \to \mathbb{Z}_n$, where $\gamma(m)$ is the remainder when m is divided by n in accordance with the division algorithm. We know that γ is a homomorphism. Of course, $\text{Ker}(\gamma) = n\mathbb{Z}$. By Theorem 14.1, we see that the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. The cosets of $n\mathbb{Z}$ are the *residue classes modulo* n. For example, taking $n = 5$, we see the cosets of $5\mathbb{Z}$ are

$$\begin{aligned}
5\mathbb{Z} &= \{\cdots, -10, -5, 0, 5, 10, \cdots\},\\
1 + 5\mathbb{Z} &= \{\cdots, -9, -4, 1, 6, 11, \cdots\},\\
2 + 5\mathbb{Z} &= \{\cdots, -8, -3, 2, 7, 12, \cdots\},\\
3 + 5\mathbb{Z} &= \{\cdots, -7, -2, 3, 8, 13, \cdots\},\\
4 + 5\mathbb{Z} &= \{\cdots, -6, -1, 4, 9, 14, \cdots\}.
\end{aligned}$$

Note that the isomorphism $\mu : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}_5$ of Theorem 14.1 assigns to each coset of $5\mathbb{Z}$ its smallest nonnegative element. That is, $\mu(5\mathbb{Z}) = 0$, $\mu(1 + 5\mathbb{Z}) = 1$, etc. ▲

It is very important that we learn how to compute in a factor group. We can multiply (add) two cosets by choosing *any* two representative elements, multiplying (adding) them and finding the coset in which the resulting product (sum) lies.

14.3 Example Consider the factor group $\mathbb{Z}/5\mathbb{Z}$ with the cosets shown above. We can add $(2 + 5\mathbb{Z}) + (4 + 5\mathbb{Z})$ by choosing 2 and 4, finding $2 + 4 = 6$, and noticing that 6 is in the coset $1 + 5\mathbb{Z}$. We could equally well add these two cosets by choosing 27 in $2 + 5\mathbb{Z}$ and -16 in $4 + 5\mathbb{Z}$; the sum $27 + (-16) = 11$ is also in the coset $1 + 5\mathbb{Z}$. ▲

The factor groups $\mathbb{Z}/n\mathbb{Z}$ in the preceding example are classics. Recall that we refer to the cosets of $n\mathbb{Z}$ as *residue classes modulo* n. Two integers in the same coset are *congruent modulo* n. This terminology is carried over to other factor groups. A factor group G/H is often called the **factor group of** G **modulo** H. Elements in the same coset of H are often said to be **congruent modulo** H. By abuse of notation, we may sometimes write $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ and think of $\mathbb{Z}_n$ as the additive group of residue classes of $\mathbb{Z}$ modulo $\langle n\rangle$, or abusing notation further, modulo n.

Factor Groups from Normal Subgroups

So far, we have obtained factor groups only from homomorphisms. Let G be a group and let H be a subgroup of G. Now H has both left cosets and right cosets, and in general, a left coset aH need not be the same set as the right coset Ha. Suppose we try to define a binary operation on left cosets by defining

$$(aH)(bH) = (ab)H \tag{4}$$

as in the statement of Theorem 14.1. Equation 4 attempts to define left coset multiplication by choosing representatives a and b from the cosets. Equation 4 is meaningless unless it gives a *well-defined* operation, independent of the representative elements a and b chosen from the cosets. The theorem that follows shows that Eq. 4 gives a well-defined binary operation if and only if H is a normal subgroup of G.

14.4 Theorem Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Proof Suppose first that $(aH)(bH) = (ab)H$ does give a well-defined binary operation on left cosets. Let $a \in G$. We want to show that aH and Ha are the same set. We use the standard technique of showing that each is a subset of the other.

Let $x \in aH$. Choosing representatives $x \in aH$ and $a^{-1} \in a^{-1}H$, we have $(xH)(a^{-1}H) = (xa^{-1})H$. On the other hand, choosing representatives $a \in aH$ and $a^{-1} \in a^{-1}H$, we see that $(aH)(a^{-1}H) = eH = H$. Using our assumption that left coset multiplication by representatives is well defined, we must have $xa^{-1} = h \in H$. Then $x = ha$, so $x \in Ha$ and $aH \subseteq Ha$. We leave the symmetric proof that $Ha \subseteq aH$ to Exercise 25.

We turn now to the converse: If H is a normal subgroup, then left coset multiplication by representatives is well-defined. Due to our hypothesis, we can simply say *cosets,* omitting *left* and *right*. Suppose we wish to compute $(aH)(bH)$. Choosing $a \in aH$ and $b \in bH$, we obtain the coset $(ab)H$. Choosing different representatives $ah_1 \in aH$ and $bh_2 \in bH$, we obtain the coset ah_1bh_2H. We must show that these are the same cosets. Now $h_1b \in Hb = bH$, so $h_1b = bh_3$ for some $h_3 \in H$. Thus

$$(ah_1)(bh_2) = a(h_1b)h_2 = a(bh_3)h_2 = (ab)(h_3h_2)$$

and $(ab)(h_3h_2) \in (ab)H$. Therefore, ah_1bh_2 is in $(ab)H$. ◆

Theorem 14.4 shows that if left and right cosets of H coincide, then Eq. 4 gives a well-defined binary operation on cosets. We wonder whether the cosets do form a group with such coset multiplication. This is indeed true.

14.5 Corollary Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$. ▲

Proof Computing, $(aH)[(bH)(cH)] = (aH)[(bc)H] = [a(bc)]H$, and similarly, we have $[(aH)(bH)](cH) = [(ab)c]H$, so associativity in G/H follows from associativity in G. Because $(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH)$, we see that $eH = H$ is the identity element in G/H. Finally, $(a^{-1}H)(aH) = (a^{-1}a)H = eH = (aa^{-1})H = (aH)(a^{-1}H)$ shows that $a^{-1}H = (aH)^{-1}$. ◆

14.6 Definition The group G/H in the preceding corollary is the **factor group** (or **quotient group**) of G by H. ■

14.7 Example Since $\mathbb{Z}$ is an abelian group, $n\mathbb{Z}$ is a normal subgroup. Corollary 14.5 allows us to construct the factor group $\mathbb{Z}/n\mathbb{Z}$ with no reference to a homomorphism. As we observed in Example 14.2, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. ▲

14.8 Example Consider the abelian group $\mathbb{R}$ under addition, and let $c \in \mathbb{R}^+$. The cyclic subgroup $\langle c \rangle$ of $\mathbb{R}$ contains as elements

$$\cdots - 3c, -2c, -c, 0, c, 2c, 3c, \cdots.$$

Every coset of $\langle c \rangle$ contains just one element x such that $0 \leq x < c$. If we choose these elements as representatives of the cosets when computing in $\mathbb{R}/\langle c \rangle$, we find that we are computing their sum modulo c as discussed for the computation in $\mathbb{R}_c$ in Section 1. For example, if $c = 5.37$, then the sum of the cosets $4.65 + \langle 5.37 \rangle$ and $3.42 + \langle 5.37 \rangle$ is the coset $8.07 + \langle 5.37 \rangle$, which contains $8.07 - 5.37 = 2.7$, which is $4.65 +_{5.37} 3.42$. Working with these coset elements x where $0 \leq x < c$, we thus see that the group $\mathbb{R}_c$ of Example 4.2 is isomorphic to $\mathbb{R}/\langle c \rangle$ under an isomorphism ψ where $\psi(x) = x + \langle c \rangle$ for all $x \in \mathbb{R}_c$. Of course, $\mathbb{R}/\langle c \rangle$ is then also isomorphic to the circle group U of complex numbers of magnitude 1 under multiplication. ▲

We have seen that the group $\mathbb{Z}/\langle n \rangle$ is isomorphic to the group $\mathbb{Z}_n$, and as a set, $\mathbb{Z}_n = \{0, 1, 3, 4, \cdots, n - 1\}$, the set of nonnegative integers less than n. Example 14.8 shows that the group $\mathbb{R}/\langle c \rangle$ is isomorphic to the group $\mathbb{R}_c$. In Section 1, we choose the notation $\mathbb{R}_c$ rather than the conventional $[0, c)$ for the half-open interval of nonnegative real numbers less than c. We did that to bring out now the comparison of these factor groups of $\mathbb{Z}$ with these factor groups of $\mathbb{R}$.

The Fundamental Homomorphism Theorem

We have seen that every homomorphism $\phi : G \to G'$ gives rise to a natural factor group (Theorem 14.1), namely, $G/\text{Ker}(\phi)$. We now show that each factor group G/H gives rise to a natural homomorphism having H as kernel.

14.9 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

Proof Let $x, y \in G$. Then

$$\gamma(xy) = (xy)H = (xH)(yH) = \gamma(x)\gamma(y),$$