Honors Algebra **Spring 2025**
HW 2: Groups **2/4/2025**

Abstract Algebra: An Integrated Approach by J.H. Silverman.
Page 53-62: 2.2, 2.6, 2.8, 2.15, 2.19, 2.21, 2.25, 2.28, 2.30, 2.33, 2.36, 2.39, 2.44, 2.45

Problem 1 (2.2)**.** Let n be a positive integer, and let S_n be the group of permutations of the set $\{1, 2, \ldots n\}$ as described in Example 2.19. Prove that S_n is a finite group, and give a formula for the order of S_n.

The symmetric group S_n consists of all possible bijections (permutations) of the set $\{1, 2, \ldots, n\}$. Since there are only finitely many elements in this set, the number of possible permutations is also finite. Thus, S_n is a finite group.

The order of S_n is determined by the number of permutations, the rearrangements, of the n elements. Thus,

$$|S_n| = n!$$

is the order of S_n.

Problem 2 (2.6)**.** Let G be a group, let g and h be elements of G, and suppose that g has order n and that h has order m.

(a) If G is an abelian group and if $\gcd(m, n) = 1$, prove that the order of gh is mn.

Since G is abelian, we have $(gh)^k = g^k h^k$ for any integer k. To find the order of gh, we need to find the smallest positive integer k such that $(gh)^k = e$.

Given that g has order n, we have $g^n = e$, and since h has order m, we have $h^m = e$. If we raise gh to the power mn, we get:

$$(gh)^{mn} = g^{mn}h^{mn} = (g^n)^m(h^m)^n = e^m e^n = e.$$

To show that mn is the smallest such exponent, assume there exists some $k < mn$ such that $(gh)^k = e$. Then:

$$g^k h^k = e.$$

Since the orders of g and h are n and m, respectively, and $\gcd(m, n) = 1$, it follows from number theory that the least common multiple of n and m is mn. Thus, the order of gh must be mn.

(b) Give an example showing that (a) need not be true if we allow $\gcd(m, n) > 1$.

Consider the abelian group $\mathbb{Z}/6\mathbb{Z}$ and let $g = 2 + 6\mathbb{Z}$ and $h = 3 + 6\mathbb{Z}$. Here, g has order 3 since $2^3 = 6 \equiv 0 \pmod 6$, and h has order 2 since $3^2 = 6 \equiv 0 \pmod 6$. However, $gh = (2 + 6\mathbb{Z}) + (3 + 6\mathbb{Z}) = 5 + 6\mathbb{Z}$, and 5 has order 6 in $\mathbb{Z}/6\mathbb{Z}$, not $3 \cdot 2 = 6$. The actual order of gh is 2, which is less than 6.

(c) Give an example of a nonabelian group showing that (a) need not be true even if we retian the requirement that $\gcd(m, n) = 1$.

Consider the symmetric group S_3, which is nonabelian. Let $g = (1\ 2)$ and $h = (1\ 2\ 3)$. The order of g is 2, and the order of h is 3. Since $\gcd(2, 3) = 1$, we check the order of gh:

$$gh = (1\ 2)(1\ 2\ 3) = (1\ 3).$$

The order of $(1\ 3)$ is 2, not $2 \cdot 3 = 6$. Hence, (a) does not necessarily hold in a nonabelian group.

(d) Again assume that G is an abelian group, and let $l = mn/\gcd(m, n)$. Porve that G has an element of order l. (*Hint:* The element gh might not have order l, so in general you'll need to take a power of g times a power of h.)

Let $d = \gcd(m, n)$. Then we can write $m = dm'$ and $n = dn'$, where $\gcd(m', n') = 1$. Define the element:

$$x = g^{m'} h^{n'}.$$

We will show that x has order $l = \frac{mn}{d} = m'n'd$.

First, compute x^l:

$$x^l = (g^{m'} h^{n'})^l = g^{m'l} h^{n'l}.$$

Since $l = m'n'd$, we substitute:

$$g^{m'l} = g^{m'm'n'd} = (g^n)^{m'n'} = e^{m'n'} = e,$$

and similarly,

$$h^{n'l} = h^{n'm'n'd} = (h^m)^{m'n'} = e^{m'n'} = e.$$

Thus, $x^l = e$, meaning that the order of x divides l.

To show that x has order exactly l, assume $x^k = e$ for some $k < l$. This would imply that $g^{m'k} = e$ and $h^{n'k} = e$. But the least common multiple of m' and n' is $m'n'$, and so k must be at least l. Thus, the order of x is l, completing the proof.

Problem 3 (2.8)**.** There are other sorts of algebraic structures that are similar to groups in that they are sets S that have a composition law

$$S \times S \longrightarrow S, \quad (s_1, s_2) \longmapsto s_1 \cdot s_2,$$

but they have fewer or different axioms than a group. In this exercise we explore two of these structures.

- The set S with its composition law is a *monoid* if it has an identity element $e \in S$ and satisfies the associative law, but elements are not required to have inverses. (See Exercise 2.19 for another example of a monoid.)
- The set S with its composition law is a *semigroup* if its composition law is associative, but it need not have an identity element or inverses. (Indeed, without an identity element, the definition of inverse doesn't even make sense.)

For each of the following sets S and composition laws $\cdot$, determine if $(S, \cdot)$ is a group, a monoid, or a semigroup.

(a) The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ with the composition law being addition.

The operation of addition is associative, meaning $(a+b)+c = a+(b+c)$ for all $a, b, c \in \mathbb{N}$. However, there is no identity element in $\mathbb{N}$ since $0 \notin \mathbb{N}$. Also inverses don't exist because there is no $b \in \mathbb{N}$ such that $a + b = e$. Therefore, $(\mathbb{N}, +)$ is a semigroup but not a monoid or a group.

(b) The set of extended natural numbers $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ with the composition law being addition.

The operation of addition is associative, and now 0 acts as an identity element since $a+0 = a$ for all $a \in \mathbb{N}_0$. In this case, additive inverses don't exist because for example, there is no $b \in \mathbb{N}_0$ such that $1 + b = 0$. Thus, $(\mathbb{N}_0, +)$ is a monoid but not a group.

(c) The set of integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ with the composition law being addition.

The operation of addition is associative, and the identity element is 0. Furthermore, every element $a \in \mathbb{Z}$ has an additive inverse $-a$ such that $a+(-a) = 0$. Hence, $(\mathbb{Z}, +)$ is a group.

(d) The set of natural numbers $\mathbb{N}$ with the composition law being multiplication.

Multiplication is associative, and the identity element is 1 since $a \cdot 1 = a$ for all $a \in \mathbb{N}$. However, there are no multiplicative inverses in $\mathbb{N}$ since $\frac{1}{a}$ is not necessarily in $\mathbb{N}$. Thus, $(\mathbb{N}, \cdot)$ is a monoid but not a group.

(e) The set of extended natural numbers $\mathbb{N}_0$ with the composition law being multiplication.

Multiplication is associative, and the identity element is still 1. However, 0 is also included, and while it does not affect the identity, it ensures the presence of absorbing elements. Since inverses don't exist for general elements, $(\mathbb{N}_0, \cdot)$ is a monoid but not a group.

(f) The set of integers $\mathbb{Z}$ with the composition law being multiplication.

Multiplication is associative, and the identity element is 1. However, not all integers have multiplicative inverses in $\mathbb{Z}$ (only 1 and -1 do). Since inverses are required for a group, $(\mathbb{Z}, \cdot)$ is a monoid but not a group.

(g) The set of integers $\mathbb{Z}$ with the composition law $m \cdot n = \max\{m, n\}$.

The operation $\max(m, n)$ is associative, meaning $\max(\max(a, b), c) = \max(a, \max(b, c))$. However, there is no identity element because no single integer e satisfies $\max(m, e) = m$ for all $m \in \mathbb{Z}$. Thus, $(\mathbb{Z}, \max)$ is a semigroup but not a monoid or a group.

(h) The set of natural numbers $\mathbb{N}$ with composition law $m \cdot n = \max\{m, n\}$

Similar to the previous case, $\max(m, n)$ is associative. Here, the identity element is 1 since $\max(m, 1) = m$ for all $m \in \mathbb{N}$. However, inverses don't exist, so $(\mathbb{N}, \max)$ is a monoid but not a group.

(i) The set of natural numbers $\mathbb{N}$ with composition law $m \cdot n = \min\{m, n\}$

The operation $\min(m, n)$ is associative, but there is no identity element that satisfies $\min(m, e) = m$ for all $m \in \mathbb{N}$. Therefore, $(\mathbb{N}, \min)$ is a semigroup but not a monoid or a group.

(j) The set natural numbers $\mathbb{N}$ with composition law $m \cdot n = mn^2$.

This operation is not associative in general since $(a \cdot b) \cdot c = (ab^2) \cdot c = (ab^2)c^2 = abc^4$ is not necessarily equal to $a \cdot (b \cdot c) = a \cdot (bc^2) = a(bc^2)^2 = ab^2c^4$. Since associativity fails, $(\mathbb{N}, \cdot)$ is not even a semigroup.

Problem 4 (2.15). (a) Let

$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

be the indicated set of 2-by-2 matrices, with composition law being matrix multiplication, as described in Example 2.21. Prove that $\mathrm{GL}_2(\mathbb{R})$ is a group.

(i) Closure

If $A, B \in \mathrm{GL}_2(\mathbb{R})$, then their determinant is nonzero, meaning their product AB also has a nonzero determinant:

$$\det(AB) = \det(A)\det(B) \neq 0.$$

Thus, $AB \in \mathrm{GL}_2(\mathbb{R})$.

(ii) Associativity

Matrix multiplication is always associative, so for all $A, B, C \in \mathrm{GL}_2(\mathbb{R})$,

$$(AB)C = A(BC).$$

(iii) Identity Element

The identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is in $\mathrm{GL}_2(\mathbb{R})$ and satisfies $AI = IA = A$ for all $A \in \mathrm{GL}_2(\mathbb{R})$.

(iv) Inverses

For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$, the determinant is nonzero, so its inverse exists and is given by:

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Since $\det(A) \neq 0$, $A^{-1} \in \mathrm{GL}_2(\mathbb{R})$.

Since all group axioms hold, $\mathrm{GL}_2(\mathbb{R})$ is a group under matrix multiplication.

(b) Let $\mathrm{SL}_2(\mathbb{R})$ be the set of 2-by-2 matrices

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

Prove that $\mathrm{SL}_2(\mathbb{R})$ is a group, where the group law is again matrix multiplication.

(i) Closure

If $A, B \in \mathrm{SL}_2(\mathbb{R})$, then their determinants are both 1. The determinant of their product is:

$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1.$$

Thus, $AB \in \mathrm{SL}_2(\mathbb{R})$.

(ii) Associativity

Since matrix multiplication is associative, for all $A, B, C \in \mathrm{SL}_2(\mathbb{R})$,

$$(AB)C = A(BC).$$

(iii) Identity Element

The identity matrix

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

has determinant $\det(I) = 1$ and belongs to $\mathrm{SL}_2(\mathbb{R})$. It satisfies $AI = IA = A$ for all $A \in \mathrm{SL}_2(\mathbb{R})$.

(iv) Inverses

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, then $ad - bc = 1$. The inverse of A is given by:

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Computing its determinant:

$$\det(A^{-1}) = (d)(a) - (-b)(-c) = ad - bc = 1.$$

Since $A^{-1} \in \mathrm{SL}_2(\mathbb{R})$, every element has an inverse.

Since all group axioms hold, $\mathrm{SL}_2(\mathbb{R})$ is a group under matrix multiplication.

Problem 5 (2.19)**.** Let X be a set. We recall from Example 2.19 that the collection of all permutations (bijective functions) $\pi : X \to X$ forms the symmetry group $\mathcal{S}_X$ of X, where the group law is composition of functions. Suppose that we instead look at the set

$$\epsilon_X = \{\text{functions} \phi : X \longrightarrow X\},$$

so we no longer require that ϕ be bijective. We can define a composition law on ϵ_X using composition of functions.

(a) Prove that ϵ_X is a monoid. (See Exercise 2.8 for the definition of monoid.)

To prove that ϵ_X is a monoid, we must verify two properties:

- Associativity

  Function composition is always associative. That is, for any $\phi, \psi, \theta \in \epsilon_X$,

  $$(\phi \circ \psi) \circ \theta = \phi \circ (\psi \circ \theta).$$

- Identity element

  The identity function $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$ is an element of ϵ_X and satisfies

  $$\mathrm{id}_X \circ \phi = \phi \circ \mathrm{id}_X = \phi$$

  for all $\phi \in \epsilon_X$.

Since ϵ_X is associative and has an identity element, it forms a monoid.

(b) If X is a finite set with n elements, prove that ϵ_X is a finite monoid and compute how many elements it has.

If X has n elements, then each function $\phi : X \to X$ assigns to each of the n elements one of n possible values in X. Thus, the number of possible functions is:

$$\text{Total elements in } \epsilon_X = n^n.$$

Since ϵ_X is finite and satisfies the monoid properties, it forms a finite monoid of order n^n.

(c) If $\#X \geq 3$, prove that ϵ_X is not commutative; i.e., show that there are elements $\phi, \psi \in \epsilon_X$ satisfying $\phi \circ \psi \neq \psi \circ \phi$

To show that ϵ_X is not commutative when $\#X \geq 3$, we provide a counterexample.

Let $X = \{a, b, c\}$, and define two functions $\phi, \psi : X \to X$ as follows:

$$\phi(a) = b, \quad \phi(b) = a, \quad \phi(c) = c$$

$$\psi(a) = a, \quad \psi(b) = c, \quad \psi(c) = b.$$

Now, we compute their compositions:

$$(\phi \circ \psi)(a) = \phi(\psi(a)) = \phi(a) = b,$$

$$(\phi \circ \psi)(b) = \phi(\psi(b)) = \phi(c) = c,$$

$$(\phi \circ \psi)(c) = \phi(\psi(c)) = \phi(b) = a.$$

On the other hand,

$$(\psi \circ \phi)(a) = \psi(\phi(a)) = \psi(b) = c,$$

$$(\psi \circ \phi)(b) = \psi(\phi(b)) = \psi(a) = a,$$

$$(\psi \circ \phi)(c) = \psi(\phi(c)) = \psi(c) = b.$$

Since $\phi \circ \psi \neq \psi \circ \phi$, ϵ_X is not commutative for $\#X \geq 3$.

Problem 6 (2.21)**.** Let G be a group, and consider the function

$$\phi : G \longrightarrow G, \qquad \phi(g) = g^{-1}$$

(a) Prove that $\phi(\phi(g)) = g$ for all $g \in G$.

By definition, $\phi(g) = g^{-1}$ for all $g \in G$. Applying ϕ again, we obtain:

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

Since ϕ takes an element to its inverse, we get:

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

By the group axioms, the inverse of g^{-1} is just g. Hence,

$$\phi(\phi(g)) = g.$$

This proves that ϕ is an involution, meaning applying it twice returns the original element.

(b) Prove that ϕ is a bijection.

Gonna show that ϕ is both injective and surjective.

Injectivity: Suppose $\phi(g_1) = \phi(g_2)$ for some $g_1, g_2 \in G$. Then:

$$g_1^{-1} = g_2^{-1}.$$

Applying the inverse operation to both sides, we obtain:

$$(g_1^{-1})^{-1} = (g_2^{-1})^{-1},$$

which simplifies to $g_1 = g_2$. Thus, ϕ is injective.

Surjectivity: For any $h \in G$, we need to find some $g \in G$ such that $\phi(g) = h$. By definition,

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

Choosing $g = h^{-1}$, we see that:

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

Since such a g exists for every $h \in G$, ϕ is surjective.

Since ϕ is both injective and surjective, it is a bijection.

(c) Prove that ϕ is a group homomorphism if and only if G is an abelian group.

The function ϕ is a group homomorphism if for all $g_1, g_2 \in G$, we have:

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2).$$

Expanding both sides using the definition of ϕ:

$$(g_1 g_2)^{-1} = g_2^{-1} g_1^{-1}.$$

For this to be equal to $\phi(g_1)\phi(g_2) = g_1^{-1} g_2^{-1}$, we require:

$$g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1}.$$

This equality holds if and only if G is abelian, meaning $g_1 g_2 = g_2 g_1$ for all $g_1, g_2 \in G$.

Thus, ϕ is a homomorphism if and only if G is abelian.

Problem 7 (2.25)**.** Let $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ be the group that we defined in Exercise 2.18.

(a) Prove that $\#\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) = 6$

The special linear group $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ consists of all 2×2 matrices with entries in $\mathbb{Z}/2\mathbb{Z}$ that have determinant equal to 1 modulo 2.

The set $\mathbb{Z}/2\mathbb{Z}$ has only two elements, $\{0, 1\}$, so the general form of a matrix in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ is:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $a, b, c, d \in \mathbb{Z}/2\mathbb{Z}$ and $\det(A) = ad - bc \equiv 1 \mod 2$.

We enumerate all possible matrices satisfying this determinant condition:

(i) If $a = 1, d = 1$, then $\det(A) = 1 - bc \equiv 1 \mod 2$ forces $bc = 0$. This gives the matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

(ii) If $a = 0, d = 0$, then $\det(A) = -bc \equiv 1 \mod 2$ is not possible since bc must be 1, but at least one of a or d is 0.

(iii) If $a = 1, d = 0$ or $a = 0, d = 1$, then $\det(A) = ad - bc \equiv 1 \mod 2$ simplifies to $bc \equiv 0 \mod 2$. This gives the matrices:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Listing all valid matrices, we find exactly six elements:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Thus, $\#\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) = 6$.

(b) Prove that $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ is isomorphic to the symmetric group $\mathcal{S}_3$. (*Hint:* Show that the matrices in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$) permute the vectors in the set $\{(1,0),(0,1),(1,1)\}$, where the coordinates of the vectors are viewed as numbers modulo 2.)

Consider the set of column vectors:

$$v_1 = \begin{pmatrix}1\\0\end{pmatrix}, \quad v_2 = \begin{pmatrix}0\\1\end{pmatrix}, \quad v_3 = \begin{pmatrix}1\\1\end{pmatrix}.$$

The matrices in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ act on this set by permutation.

Computing the action of each matrix on the basis vectors:

(i) The identity matrix $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ fixes all vectors.

(ii) The matrix $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ sends:

$$v_1 \mapsto v_3, \quad v_2 \mapsto v_2, \quad v_3 \mapsto v_1.$$

This corresponds to the transposition (13).

(iii) The matrix $\begin{pmatrix}1&0\\1&1\end{pmatrix}$ sends:

$$v_1 \mapsto v_1, \quad v_2 \mapsto v_3, \quad v_3 \mapsto v_2.$$

This corresponds to the transposition (23).

(iv) The matrix $\begin{pmatrix}1&1\\1&0\end{pmatrix}$ sends:

$$v_1 \mapsto v_2, \quad v_2 \mapsto v_1, \quad v_3 \mapsto v_3.$$

This corresponds to the transposition (12).

(v) The matrix $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ sends:

$$v_1 \mapsto v_3, \quad v_2 \mapsto v_1, \quad v_3 \mapsto v_2.$$

This corresponds to the 3-cycle (132).

(vi) The matrix $\begin{pmatrix}0&1\\1&0\end{pmatrix}$ sends:

$$v_1 \mapsto v_2, \quad v_2 \mapsto v_3, \quad v_3 \mapsto v_1.$$

This corresponds to the 3-cycle (123).

Since these matrices permute the three vectors exactly as the elements of the symmetric group $\mathcal{S}_3$ do, we have a group homomorphism from $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ to $\mathcal{S}_3$. Because both groups have exactly six elements, and the mapping is bijective, it is an isomorphism.

Thus,

$$\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \cong \mathcal{S}_3.$$

Problem 8 (2.28)**.** Let G be a group, and let $H \subset G$ be a subset of G. Prove that H is a subgroup if and only if it has the following two properties:

1. $H \neq \emptyset$
2. For every $h_1, h_2 \in H$, the product $h_1 \cdot h_2^{-1}$ is in H.

We need to prove that H is a subgroup of G if and only if it satisfies the given conditions.

($\Rightarrow$) Suppose H is a subgroup of G.

- Since H is a subgroup, it contains the identity element e of G. Thus, H is nonempty.
- Since H is closed under multiplication and contains inverses, for every $h_1, h_2 \in H$, we have $h_2^{-1} \in H$.
- Since subgroups are closed under multiplication, the element $h_1 \cdot h_2^{-1}$ must also be in H.

Hence, H satisfies both conditions.

($\Leftarrow$) Suppose H satisfies the given conditions.

- Since $H \neq \emptyset$, there exists at least one element $h \in H$.
- Choosing $h_1 = h$ and $h_2 = h$, the second condition implies $h \cdot h^{-1} = e \in H$, so H contains the identity.
- To show closure under inverses, let $h \in H$. Taking $h_1 = e$ and $h_2 = h$, we get $e \cdot h^{-1} = h^{-1} \in H$. Thus, H is closed under taking inverses.
- Finally, for closure under multiplication, let $h_1, h_2 \in H$. Since H contains inverses, we can replace h_2 with h_2^{-1} in the given condition, giving us $h_1 \cdot (h_2^{-1})^{-1} = h_1 \cdot h_2 \in H$.

Since H contains the identity, is closed under inverses, and is closed under multiplication, it is a subgroup of G.

The two given conditions are necessary and sufficient for H to be a subgroup of G.

Problem 9 (2.30)**.** This exercise generalizes the notion of the cyclic subgroup generated by an element of a group as described in Example 2.37. Let G be a group, and let $S \subseteq G$ be a subset of G. The *subgroup of G generated by S*, which we denote by $\langle S \rangle$, is the intersection of all of the subgroups of G that contain S; i.e.,

$$\langle S \rangle = \bigcap_{\substack{S \subseteq H \subset G \\ H \text{ is a subgroup of } G}} H.$$

(a) Prove that $\langle S \rangle$ is not the empty set.

Note that G is a group, and hence contains the identity element e. Every subgroup of G must contain e, including all subgroups that contain S. Since $\langle S \rangle$ is defined as the intersection of all such subgroups, it must also contain e. Thus, $\langle S \rangle \neq \emptyset$.

(b) Prove that $\langle S \rangle$ is a subgroup of G.

Recall that a subset H of G is a subgroup if it satisfies the following:

(i) It contains the identity element.

(ii) It is closed under the group operation.

(iii) It is closed under inverses.

Since each subgroup containing S is a subgroup of G, it must satisfy these properties. The intersection of any collection of subgroups is itself a subgroup, since all properties are preserved under intersection. Since $\langle S \rangle$ is defined as such an intersection, it must also be a subgroup of G.

(c) Suppose that $K \subseteq G$ is a subgroup of K and that $S \subseteq K$. Prove that $K \subset \langle S \rangle$. Thus $\langle S \rangle$ is often described as being the smallest subgroup of G that contains the set S.

Suppose that K is a subgroup of G containing S. By definition, $\langle S \rangle$ is the intersection of all subgroups containing S. Since K is one of these subgroups, it follows that $\langle S \rangle \subseteq K$. Therefore, $\langle S \rangle$ is the smallest subgroup of G containing S.

(d) Let T be the set of inverses of the elements in S; i.e.,

$$T = \{g^{-1} : g \in S\}$$

Prove that $\langle S \rangle$ is equal to the following set of products:

$$\langle S \rangle = \{g_1 g_2 \cdots g_n : n \geq 0 \text{ and } g_1, \ldots, g_n \in S \cup T\}$$

If $G = \langle S \rangle$, then we say that S generates G, or that S is a generating set for G.

Define

$$H = \{g_1 g_2 \cdots g_n : n \geq 0 \text{ and } g_1, g_2, \ldots, g_n \in S \cup T\}.$$

We will show that $H = \langle S \rangle$.

- First, note that H is a subgroup: It contains the identity element ($n = 0$ gives the identity), it is closed under multiplication by construction, and since T contains the inverses of elements in S, H is closed under taking inverses.
- Since H contains S and is a subgroup of G, it must contain $\langle S \rangle$, the smallest subgroup containing S, so $\langle S \rangle \subseteq H$.
- Conversely, $\langle S \rangle$ must be closed under multiplication and taking inverses, so it contains all finite products of elements from $S \cup T$, meaning $H \subseteq \langle S \rangle$.

Since we have both $\langle S \rangle \subseteq H$ and $H \subseteq \langle S \rangle$, it follows that $H = \langle S \rangle$, completing the proof.

Problem 10 (2.33)**.** Let G be a group, let $A \subseteq G$ and $B \subseteq G$ be subgroups of G, and let ϕ be the map

$$\phi : A \times B \longrightarrow G, \qquad \phi(a, b) = ab$$

(a) Prove that $A \cap B = \{e\}$ if and only if the map ϕ is an injective map of sets.

Let's look at both directions:

$\Longleftarrow$ Suppose ϕ is injective. If there exists some $x \in A \cap B$ with $x \neq e$, then $\phi(x, e) = x$ and $\phi(e, x) = x$, contradicting injectivity since $(x, e) \neq (e, x)$. Thus, $A \cap B = \{e\}$.

$\Longrightarrow$ Conversely, assume $A \cap B = \{e\}$ and suppose $\phi(a_1, b_1) = \phi(a_2, b_2)$. Then $a_1 b_1 = a_2 b_2$, which rearranges to $a_1 a_2^{-1} = b_2 b_1^{-1}$. Since $a_1 a_2^{-1} \in A$ and $b_2 b_1^{-1} \in B$, and the only element common to both is e, we conclude $a_1 = a_2$ and $b_1 = b_2$, proving injectivity.

(b) We can turn $A \times B$ into a group by using the group operation

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2)$$

(See Section 2.6 for further details on product groups.) Prove that the map ϕ is a homomorphism of groups if and only if every element of A commutes with every element of B.

The map ϕ is a homomorphism if for all $(a_1, b_1), (a_2, b_2) \in A \times B$, we have:

$$\phi((a_1, b_1) \cdot (a_2, b_2)) = \phi(a_1, b_1) \cdot \phi(a_2, b_2).$$

Expanding both sides:

$$\phi(a_1 a_2, b_1 b_2) = (a_1 a_2)(b_1 b_2).$$

On the other hand,

$$\phi(a_1, b_1) \cdot \phi(a_2, b_2) = (a_1 b_1)(a_2 b_2).$$

For these to be equal, we require that multiplication can be rearranged as:

$$(a_1 b_1)(a_2 b_2) = (a_1 a_2)(b_1 b_2).$$

This holds if and only if $a_2 b_1 = b_1 a_2$ for all $a_2 \in A$ and $b_1 \in B$, which means every element of A commutes with every element of B.

Problem 11 (2.36)**.** Let G be a group, and let $g \in G$. The *centralizer of* g, denoted $Z_G(g)$, is the set of elements of G that commute with g; i.e.,

$$Z_G(g) = \{g' \in G : gg' = g'g\}$$

(a) Prove that $Z_G(g)$ is a subgroup of G.

We prove that $Z_G(g)$ is a subgroup of G by checking the subgroup criteria:

- The identity element e satisfies $eg = ge$, so $e \in Z_G(g)$.

- If $g_1, g_2 \in Z_G(g)$, then $gg_1 = g_1g$ and $gg_2 = g_2g$. Multiplying these gives

$$g(g_1g_2) = (gg_1)g_2 = (g_1g)g_2 = g_1(gg_2) = g_1(g_2g) = (g_1g_2)g,$$

so $g_1g_2 \in Z_G(g)$.

- If $g' \in Z_G(g)$, then $gg' = g'g$. Taking inverses, we get

$$g'^{-1}g^{-1} = g^{-1}g'^{-1}.$$

Since inverses exist in G, we conclude $g'^{-1} \in Z_G(g)$.

Thus, $Z_G(g)$ is a subgroup of G.

(b) Compute the centralizer $Z_G(g)$ for the following groups and elements:

(i) $G = \mathcal{D}_4$ and g is rotation by $90°$

$Z_G(g)$ consists of elements that commute with g. These elements are the rotations (0, 90, 180, 270 degrees), forming the cyclic subgroup $\{e, g, g^2, g^3\}$.

(ii) $G = \mathcal{D}_4$ and f is a flip fixing two of the vertices of the square.

$Z_G(f)$ consists of elements that commute with f. These include e, f, the 180-degree rotation, and the other flip along the perpendicular axis.

(iii) $G = \mathrm{GL}_2(\mathbb{R})$ and $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$

$Z_G(g)$ consists of all matrices that commute with g. These are precisely the diagonal and block diagonal matrices of the form

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix},$$

meaning $Z_G(g)$ is the set of all such matrices in $\mathrm{GL}_2(\mathbb{R})$.

Problem 12 (2.39)**.** Let G be a group, and let $K \subseteq H \subseteq G$ be subgroups. We may thus view K as a subgroup of G or as a subgroup of H. We also recall that the index of a subgroup is its number of distinct cosets; see Definition 2.49.

(a) If G is finite, prove the *Index Multiplication Rule*

$$(G : K) = (G : H)(H : K)$$

(*Hint.* Use (2.11) in Definition 2.49.)

To prove the Index Multiplication Rule, we analyze the number of cosets:

- By definition, $(G : H)$ is the number of left cosets of H in G, and $(H : K)$ is the number of left cosets of K in H.
- Each left coset of H in G can be written as gH for some $g \in G$.

- Each left coset of K in H can be written as hK for some $h \in H$.
- Consider the collection of left cosets of K in G, which are of the form gK for some $g \in G$.
- Since each coset gH can be subdivided into $(H : K)$ cosets of K in G, we obtain:

$$(G : K) = (G : H)(H : K).$$

(b) *Challenge Problem.* Prove that the Index Multiplication Rule (2.13) is true even if G, H, and K are allowed to be infinite groups, provided that we assume that $(G : K)$ is finite. (*Hint.* Take cosets for H in G and cosets for K in H, and use them to build cosets for K in G.)

We extend the proof to the case where G, H, and K are infinite, assuming that $(G : K)$ is finite.

- Define the set of left cosets of H in G as $\{g_iH : i \in I\}$, where I is an index set of size $(G : H)$.
- Similarly, define the set of left cosets of K in H as $\{h_jK : j \in J\}$, where J is an index set of size $(H : K)$.
- Each element of G can be written uniquely as g_ih_jk for some g_iH, h_jK, and $k \in K$.
- Therefore, the number of left cosets of K in G is the product of the number of left cosets of H in G and the number of left cosets of K in H:

$$(G : K) = (G : H)(H : K).$$

This holds even when G, H, K are infinite, provided $(G : K)$ is finite.

Problem 13 (2.44)**.** Let G_1 and G_2 be groups, and let $p_1, p_2, \iota_1, \iota_2$ be the projection and inclusion maps described in Section 2.6.

(a) Prove that p_1 and p_2 are homomorphisms.

The projection maps $p_1 : G_1 \times G_2 \to G_1$ and $p_2 : G_1 \times G_2 \to G_2$ are homomorphisms since for any $(a_1, b_1), (a_2, b_2) \in G_1 \times G_2$, we have:

$$p_1((a_1, b_1)(a_2, b_2)) = p_1(a_1a_2, b_1b_2) = a_1a_2 = p_1(a_1, b_1)p_1(a_2, b_2).$$

A similar argument holds for p_2.

(b) Prove that ι_1 and ι_2 are homomorphisms.

The inclusion maps $\iota_1 : G_1 \to G_1 \times G_2$ and $\iota_2 : G_2 \to G_1 \times G_2$ are homomorphisms since for any $a_1, a_2 \in G_1$, we have:

$$\iota_1(a_1a_2) = (a_1a_2, e) = (a_1, e)(a_2, e) = \iota_1(a_1)\iota_1(a_2).$$

A similar argument holds for ι_2.

(c) Compute the following compositions of these maps:

$p_1 \circ \iota_1(a)$	$p_2 \circ \iota_1(a)$	$p_1 \circ \iota_2(b)$	$p_2 \circ \iota_2(b)$
a	e	e	b
$\iota_1 \circ p_1(a,b)$	$\iota_2 \circ p_1(a,b)$	$\iota_1 \circ p_2(a,b)$	$\iota_2 \circ p_2(a,b)$
(a,e)	(e,e)	(e,e)	(e,b)

Problem 14 (2.45)**.** Let G_1 and G_2 be groups, and let $p_1, p_2, \iota_1, \iota_2$ be the projection and inclusion maps described in Section 2.6.

(a) Suppose that G is some other group and that we are given group homomorphisms

$$\psi_1 : G \longrightarrow G_1 \quad \psi_2 : G \longrightarrow G_2$$

Prove that there exists a unique group homomorphism

$$\phi : G \longrightarrow G_1 \times G_2$$

with the property that

$$p_1(\phi(g)) = \psi_1(g) \quad p_2(\phi(g)) = \psi_2(g) \quad \text{for all } g \in G.$$

Define $\phi : G \to G_1 \times G_2$ by

$$\phi(g) = (\psi_1(g), \psi_2(g)).$$

We verify that ϕ is a group homomorphism. For any $g, h \in G$,

$$\phi(gh) = (\psi_1(gh), \psi_2(gh)) = (\psi_1(g)\psi_1(h), \psi_2(g)\psi_2(h)) = \phi(g)\phi(h),$$

showing that ϕ is a homomorphism. Uniqueness follows because any such ϕ must satisfy $p_1(\phi(g)) = \psi_1(g)$ and $p_2(\phi(g)) = \psi_2(g)$, uniquely determining ϕ.

(b) Suppose that G is an abelian group, and suppose that we are given group homomorphisms

$$\lambda_1 : G_1 \longrightarrow G \quad \text{and} \quad \lambda_2 : G_2 \longrightarrow G.$$

Prove that there exists a unique group homomorphism

$$\mu : G_1 \times G_2 \longrightarrow G$$

with the property that for all $g_1 \in G_1$ and all $g_2 \in G_2$ we have

$$\mu(\iota_1(g_1)) = \lambda_1(g_1) \quad \text{and} \quad \mu(\iota_2(g_2)) = \lambda_2(g_2).$$

(*Hint.* First show that (2.14) uniquely determines μ as a map of sets, and then verify that μ is a homomorphism.)

Define $\mu : G_1 \times G_2 \to G$ by setting

$$\mu(g_1, g_2) = \lambda_1(g_1)\lambda_2(g_2).$$

This function is uniquely determined because for any $(g_1, g_2) \in G_1 \times G_2$,

$$\mu(\iota_1(g_1)) = \lambda_1(g_1), \quad \mu(\iota_2(g_2)) = \lambda_2(g_2).$$

To show that μ is a homomorphism, let $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$. Since G is abelian,

$$\mu((g_1, g_2)(h_1, h_2)) = \mu(g_1h_1, g_2h_2) = \lambda_1(g_1h_1)\lambda_2(g_2h_2).$$

Using the homomorphism property of λ_1 and λ_2,

$$\lambda_1(g_1h_1) = \lambda_1(g_1)\lambda_1(h_1), \quad \lambda_2(g_2h_2) = \lambda_2(g_2)\lambda_2(h_2).$$

Since G is abelian, we get

$$\mu(g_1, g_2)\mu(h_1, h_2) = \lambda_1(g_1)\lambda_2(g_2)\lambda_1(h_1)\lambda_2(h_2) = \lambda_1(g_1)\lambda_1(h_1)\lambda_2(g_2)\lambda_2(h_2),$$

which equals $\mu((g_1, g_2)(h_1, h_2))$, proving that μ is a homomorphism.

(c) Continuing with the notation from (b), let Γ be a non-abelian group, let

$$G_1 = G_2 = G = \Gamma,$$

and let

$$\lambda_1 : G_1 \longrightarrow G \text{ and } \lambda_2 : G_2 \longrightarrow G \text{ both be the identity map}$$

Prove that there does *not* exist a homomorphism $\mu : G_1 \times G_2 \longrightarrow G$ satisfying (2.14). (*Hint.* As noted in (b), the map μ exists as a map of sets, so your task is to show that μ is not a group homomorphism.)

Bonus: Generalize Exercise 2.45 to a product $G_1 \times G_2 \times \cdots \times G_n$ of more than two groups.

Suppose $G_1 = G_2 = G = \Gamma$ and λ_1, λ_2 are identity maps. Then, for all $g_1, g_2 \in \Gamma$,

$$\mu(g_1, g_2) = g_1g_2.$$

If μ were a homomorphism, then for all $g_1, g_2, h_1, h_2 \in \Gamma$,

$$\mu((g_1, g_2)(h_1, h_2)) = \mu(g_1h_1, g_2h_2) = g_1h_1g_2h_2.$$

However, applying μ separately,

$$\mu(g_1, g_2)\mu(h_1, h_2) = (g_1g_2)(h_1h_2).$$

Since Γ is non-abelian, in general $g_2h_1 \neq h_1g_2$, meaning the two expressions do not always match. Thus, μ is not a homomorphism.