Introduction to Abstract Algebra I: Homework 2

Due on October 15, 2025 at 23:59

Victor Ostrik

Hashem A. Damrah
UO ID: 952102243

Exercise 2.10. Let n be a positive integer and let $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.

(i) Show that $\langle n\mathbb{Z}, +\rangle$ is a group.

(ii) Show that $\langle n\mathbb{Z}, +\rangle \cong \langle \mathbb{Z}, +\rangle$.

Solution to (i). We verify the group axioms for $\langle n\mathbb{Z}, +\rangle$.

Let $a, b \in n\mathbb{Z}$. Then $a = nm$ and $b = nk$ for some $m, k \in \mathbb{Z}$. Hence,

$$a + b = nm + nk = n(m + k).$$

Since $m + k \in \mathbb{Z}$, it follows that $a + b \in n\mathbb{Z}$.

Addition in $\mathbb{Z}$ is associative, and $n\mathbb{Z}$ inherits this property. Thus, for all $a, b, c \in n\mathbb{Z}$,

$$(a + b) + c = a + (b + c).$$

The additive identity is 0, since for any $a \in n\mathbb{Z}$,

$$a + 0 = a.$$

For any $a = nm \in n\mathbb{Z}$, the additive inverse is $-a = n(-m)$, because

$$a + (-a) = nm + n(-m) = n(m - m) = 0.$$

Therefore, all group axioms are satisfied, and $\langle n\mathbb{Z}, +\rangle$ is a group. □

Solution to (ii). Define a map $\varphi : \mathbb{Z} \to n\mathbb{Z}$ by $\varphi(m) = nm$, for all $m \in \mathbb{Z}$. We show that φ is an isomorphism.

For any $m_1, m_2 \in \mathbb{Z}$,

$$\varphi(m_1 + m_2) = n(m_1 + m_2) = nm_1 + nm_2 = \varphi(m_1) + \varphi(m_2).$$

Hence, φ preserves addition.

Suppose $\varphi(m_1) = \varphi(m_2)$. Then $nm_1 = nm_2$, and since $n \neq 0$, we may divide by n to obtain $m_1 = m_2$. Thus, φ is injective.

For any $a \in n\mathbb{Z}$, there exists $k \in \mathbb{Z}$ such that $a = nk$. Then $\varphi(k) = nk = a$, so φ is surjective.

Since φ is an isomorphism, it follows that $\langle n\mathbb{Z}, +\rangle \cong \langle \mathbb{Z}, +\rangle$. □

Exercise 2.19. Let S be the set of all real numbers except -1. Define $*$ on S by

$$a * b = a + b + ab.$$

(i) Show that $*$ gives a binary operation on S.

(ii) Show that $\langle S, *\rangle$ is a group.

(iii) Find the solution of the equation $2 * x * 3 = 7$ in S.

Solution to (i). We need to show that for any $a, b \in S$, the result of the operation $a * b$ is also in S.

Let $a, b \in S$. Then, $a * b = a + b + ab$. We need to check that $a * b \neq -1$. Suppose for contradiction that $a * b = -1$. Then, $a + b + ab = -1$. Rearranging gives $ab + a + b + 1 = 0$, which can be factored as $(a + 1)(b + 1) = 0$.

Since $a, b \in S$, we have $a \neq -1$ and $b \neq -1$, so neither factor can be zero. This is a contradiction. Therefore, $a * b \neq -1$, and thus $a * b \in S$.

Hence, $*$ is a binary operation on S. □

Solution to (ii). We verify the group axioms for $\langle S, * \rangle$.

As shown in part (i), for any $a, b \in S$, $a * b \in S$.

For any $a, b, c \in S$,

$$(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c.$$

Expanding this gives

$$a + b + ab + c + ac + bc + abc.$$

Similarly,

$$a * (b * c) = a * (b + c + bc) = a + (b + c + bc) + a(b + c + bc).$$

Expanding this also gives

$$a + b + c + bc + ab + ac + abc.$$

Since both expressions are equal, $*$ is associative.

We need to find an element $e \in S$ such that for all $a \in S$, $a * e = e * a = a$. Let $e = 0$. Then,

$$a * 0 = a + 0 + a \cdot 0 = a,$$

and

$$0 * a = 0 + a + 0 \cdot a = a.$$

Thus, 0 is the identity element.

Fix $a \in S$. We want to find a $b \in S$ with $a * b = 0$. Solving the equation $a + b + ab = 0$, we get $(a + 1)(b + 1) = 1$. Thus $b + 1 = 1/(a + 1)$, so

$$b = \frac{1}{a + 1} - 1 = -\frac{a}{a + 1}.$$

Since $a \neq -1$ the denominator $a + 1 \neq 0$, so this b is well-defined and satisfies $b \neq -1$. Notice that $b \neq -1$, since that would imply that $-a/(a + 1) = -1$, which gives us $0 = 1$, which is a contradiction. Hence every element has a two-sided inverse in S.

Since all group axioms are satisfied, $\langle S, * \rangle$ is a group. □

Solution to (iii). We need to solve the equation $2 * x * 3 = 7$ in S. First, we compute $2 * x$:

$$2 * x = 2 + x + 2x = x + 2 + 2x = 3x + 2.$$

Next, we compute $(2 * x) * 3$:

$$(3x + 2) * 3 = (3x + 2) + 3 + (3x + 2) \cdot 3 = 3x + 2 + 3 + 9x + 6 = 12x + 11.$$

We set this equal to 7:

$$12x + 11 = 7.$$

Solving for x, we get

$$12x = -4 \Rightarrow x = -\frac{1}{3}.$$

Since $-1/3 \in S$, the solution is $x = -1/3$. □

Exercise 2.28. An element $a \neq e$ in a group is said to have order 2 if $a * a = e$. Prove that if G is a group and $a \in G$ has order 2, then for any $b \in G$, $b' * a * b$ also has order 2.

Solution. Assume $a \neq e$ is an element of order 2 in the group G, i.e., $a * a = e$. Then, for any $b \in G$, we compute the square of the element $b' * a * b$:

$$(b' * a * b) * (b' * a * b) = b' * a * (b * b') * a * b = b' * a * a * b = b' * b = e.$$

Thus, $(b' * a * b)$ has order 2. □

Exercise 2.29. Show that if G is a finite group with identity e and with an even number of elements, then there is $a \neq e$ in G such that $a * a = e$.

Solution. Let G be a finite group with identity e and an even number of elements. Consider the set $G \setminus \{e\}$, which has an odd number of elements.

For each element $a \in G \setminus \{e\}$, consider its inverse a'. If $a \neq a'$, then we can pair a with a'. Each such pair contributes two distinct elements to the set. Since the total number of elements in $G \setminus \{e\}$ is odd, there must be at least one element that is its own inverse, i.e., an element a such that $a = a'$.

For this element, we have $a * a = e$. Since $a \neq e$, we have found an element in G such that $a * a = e$. □

Exercise 2.30. Let $\mathbb{R}^*$ be the set of all real numbers except 0. Define $*$ on $\mathbb{R}^*$ by letting $a * b = |a|b$.

(i) Show that $*$ gives an associative binary operation on $\mathbb{R}^*$.

(ii) Show that there is a left identity for $*$ and a right inverse for each element in $\mathbb{R}^*$.

(iii) Is $\mathbb{R}^*$ with this binary operation a group?

(iv) Explain the significance of this exercise.

Solution to (i). We need to show that for any $a, b \in \mathbb{R}^*$, the result of the operation $a * b$ is also in $\mathbb{R}^*$.

Let $a, b \in \mathbb{R}^*$. Then, $a * b = |a|b$. Since $|a|> 0$ and $b \neq 0$, it follows that $|a|b \neq 0$. Thus, $a * b \in \mathbb{R}^*$.

Next, we verify associativity. For any $a, b, c \in \mathbb{R}^*$,

$$(a * b) * c = (|a|b) * c = ||a|b|c = |a||b|c.$$

Similarly,

$$a * (b * c) = a * (|b|c) = |a|(|b|c) = |a||b|c.$$

Since both expressions are equal, $*$ is associative.

Therefore, $*$ is an associative binary operation on $\mathbb{R}^*$. □

Solution to (ii). We need to find a left identity element $e \in \mathbb{R}^*$ such that for all $a \in \mathbb{R}^*$, $e * a = a$. Let $e = 1$. Then,

$$e * a = 1 * a = |1|a = a.$$

Thus, 1 is a left identity.

Next, we need to find a right inverse for each element $a \in \mathbb{R}^*$. We want to find $b \in \mathbb{R}^*$ such that $a * b = e$. Using the left identity found above, we have:

$$a * b = |a|b = 1.$$

Solving for b, we get:

$$b = \frac{1}{|a|}.$$

Since $|a|> 0$, it follows that $b \neq 0$, and thus $b \in \mathbb{R}^*$. Therefore, every element in $\mathbb{R}^*$ has a right inverse.

Hence, there is a left identity and a right inverse for each element in $\mathbb{R}^*$. □

Solution to (iii). To determine if $\mathbb{R}^*$ with the operation $*$ is a group, we need to check if it satisfies all group axioms.

We have already shown that $*$ is an associative binary operation on $\mathbb{R}^*$, and that there is a left identity element (1) and a right inverse for each element.

However, we need to check if the left identity is also a right identity. For any $a \in \mathbb{R}^*$,

$$a * e = a * 1 = |a| \cdot 1 = |a|.$$

Since $|a|$ is not necessarily equal to a (for example, if $a = -2$, then $|a|= 2$), the left identity is not a right identity.

Therefore, $\mathbb{R}^*$ with this binary operation does not satisfy all the group axioms, and hence it is not a group. □

Solution to (iv). The significance of this exercise is to illustrate that having a left identity and right inverses for each element does not guarantee that a set with a binary operation forms a group. The failure of the left identity to also be a right identity shows that the group axioms are not fully satisfied. This shows the importance of verifying all group properties when determining if a structure is indeed a group. □

Exercise 2.31. If $*$ is a binary operation on a set S, an element x of S is an *idempotent for* $*$ if $x * x = x$. Prove that a group has exactly one idempotent element. (You may use any theorems proved so far in the text.)

Solution. Let G be a group with identity element e. We first show that e is an idempotent element. Obviously, $e * e = e$.

Now, suppose there is another idempotent element $x \in G$ such that $x * x = x$. We will show that $x = e$.

Since G is a group, every element has an inverse. Let x' be the inverse of x. Then,

$$x' * (x * x) = x' * x.$$

Using associativity, we have $(x' * x) * x = e * x = x$. But since $x' * x = e$, we have $e * x = x$. Therefore, $x = e$.

Thus, the only idempotent element in the group G is the identity element e. Hence, a group has exactly one idempotent element. □

Exercise 2.32. Show that every group G with identity e and such that $x * x = e$ for all $x \in G$ is abelian. [Hint: Consider $(a * b) * (a * b)$.]

Solution. Let $a, b \in G$. Since $x * x = e$ for all $x \in G$, each element is its own inverse; i.e. $x' = x$ for every $x \in G$.

Consider $(a * b) * (a * b)$. By hypothesis $(a * b) * (a * b) = e$, so

$$(a * b)' = (a * b).$$

On the other hand, the general inverse formula in any group gives $(a * b)' = b' * a'$. Using $x' = x$ for a and b we obtain

$$(a * b)' = b' * a' = b * a.$$

Combining the two expressions for $(a * b)'$ yields $a * b = b * a$. Thus, G is abelian. □

Exercise 2.33. Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a mathematical induction proof that $(a * b)^n = (a^n) * (b^n)$ for all $a, b \in G$.

Solution. We will prove by induction on n that for all $a, b \in G$, $(a * b)^n = (a^n) * (b^n)$.

For the base case, we have $n = 1$, which gives us

$$(a * b)^1 = a * b.$$

Also,

$$a^1 * b^1 = a * b.$$

Thus, the base case holds.

Assume that the statement holds for some $k \in \mathbb{Z}^+$, i.e., assume that

$$(a * b)^k = (a^k) * (b^k).$$

We need to show that it holds for $k+1$. Consider:

$$(a*b)^{k+1} = (a*b)^k * (a*b).$$

By the inductive hypothesis, we have:

$$(a*b)^{k+1} = ((a^k)*(b^k))*(a*b).$$

Since G is abelian, we can rearrange the terms:

$$(a*b)^{k+1} = (a^k*a)*(b^k*b) = a^{k+1}*b^{k+1}.$$

Thus, by the principle of mathematical induction, the statement holds for all $n \in \mathbb{Z}^+$. □

Exercise 2.34. Suppose that G is a group and $a, b \in G$ satisfy $a*b = b*a'$ where as usual, a' is the inverse for a. Prove that $b*a = a'*b$.

Solution. Given that $a*b = b*a'$, we want to show that $b*a = a'*b$.

Starting from the given equation, we can multiply both sides on the left by a':

$$a'*(a*b) = a'*(b*a').$$

Using associativity, we have:

$$(a'*a)*b = a'*b*a'.$$

Simplifying, we get:

$$b = a'*b*a'.$$

Now, we can multiply both sides on the right by a:

$$b*a = (a'*b*a')*a.$$

Again, using associativity, we have:

$$b*a = a'*b*(a'*a).$$

Since $a'*a = e$, this simplifies to:

$$b*a = a'*b.$$

Thus, we have shown that $b*a = a'*b$. □

Exercise 2.36. Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists $n \in \mathbb{Z}^+$ such that $a^n = e$. See Exercise 33 for the meaning of a^n. [Hint: Consider $e, a, a^2, a^3, \cdots, a^m$, where m is the number of elements in G, and use the cancellation laws.]

Solution. Let G be a finite group with m elements. Consider the sequence of elements:

$$e, a, a^2, a^3, \cdots, a^m.$$

Since G has only m elements, by the pigeonhole principle, at least two of these elements must be equal. Thus, there exist integers i and j with $0 \le i < j \le m$ such that:

$$a^i = a^j.$$

Using the cancellation law (which holds in groups), we can multiply both sides on the left by $(a^i)'$, the inverse of a^i, to obtain:

$$e = a^{j-i}.$$

Letting $n = j - i$, we have found a positive integer n such that $a^n = e$. Thus, for any element $a \in G$, there exists $n \in \mathbb{Z}^+$ such that $a^n = e$. □