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

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 $a + b \in n\mathbb{Z}$, so $n\mathbb{Z}$ is closed under addition.

Because addition in $\mathbb{Z}$ is associative, $n\mathbb{Z}$ 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 will show that φ is an isomorphism.

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

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

so φ preserves addition and is therefore a homomorphism.

Suppose $\varphi(m_1) = \varphi(m_2)$. Then $nm_1 = nm_2$, and subtracting gives $n(m_1 - m_2) = 0$. Since $n \neq 0$ and $\mathbb{Z}$ has no zero divisors, we conclude that $m_1 - m_2 = 0$, or $m_1 = m_2$. 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.

Therefore, φ is a bijective homomorphism, and hence an isomorphism. We conclude 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). Let $a, b \in S$, so $a \neq -1$ and $b \neq -1$. If $a * b = -1$ then $a + b + ab = -1$, which rearranges to

$$ab + a + b + 1 = (a + 1)(b + 1) = 0.$$

But $a + 1 \neq 0$ and $b + 1 \neq 0$, so this is impossible. Hence $a * b \neq -1$, and therefore $a * b \in S$. Thus $*$ is a binary operation on S. □

Solution to (ii). We first check that associativity holds. Notice that for any $a, b, c \in S$, we have

$$\begin{aligned}(a * b) * c &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a * (b * c).\end{aligned}$$

So $(a * b) * c = a * (b * c)$. Thus $*$ is associative.

The identity element is 0, since for any $a \in S$,

$$a * 0 = a + 0 + a \cdot 0 = a \quad \text{and} \quad 0 * a = 0 + a + 0 \cdot a = a..$$

Now fix $a \in S$ and solve $a * b = 0$. The equation $a + b + ab = 0$ can be rewritten as $(a+1)(b+1) = 1$, hence

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

Since $a \neq -1$ the denominator $a + 1 \neq 0$, so this b is well-defined and satisfies $b \neq -1$. Notice that

$$-\frac{a}{a+1} = -1 \Leftrightarrow a = a + 1 \Leftrightarrow 1 = 0,$$

which is false. Therefore, $b \in S$. Because $*$ is commutative, this element is both a left and right inverse of a. Therefore every element of S has a two-sided inverse.

Since $\langle S, * \rangle$ has associativity, an identity, and two-sided inverses, $\langle S, * \rangle$ is a group. $\square$

Solution to (iii). To solve $2 * x * 3 = 7$ let us first compute $2 * x = 2 + x + 2x = 3x + 2$. Then

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

Setting $12x + 11 = 7$ gives $12x = -4$, so $x = -1/3$. Since $-1/3 \neq -1$, this solution lies in S. $\square$

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. Let $a \neq e$ be an element of order 2 in the group G, so $a * a = e$. For any $b \in G$, we consider the element $b' * a * b$ and compute its square:

$$\begin{aligned}
(b' * a * b) * (b' * a * b) &= b' * a * (b * b') * a * b \\
&= b' * a * e * a * b \\
&= b' * a * a * b \\
&= b' * e * b \\
&= b' * b \\
&= e.
\end{aligned}$$

Hence, $(b' * a * b)$ has order 2.

Therefore, for any $b \in G$, the element $b' * a * b$ also has order 2. In other words, conjugation by b preserves the order of elements in G. $\square$

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 $a \in G \setminus \{e\}$, let a' denote its inverse. If $a \neq a'$, we can pair a with a', and each such pair contributes two distinct elements to the set. These pairs together account for an even number of elements.

Since $G \setminus \{e\}$ has an odd number of elements, at least one element must remain unpaired. For this element a, we must have $a = a'$, that is, $a * a = e$.

Because $a \neq e$, we have found a non-identity element $a \in G$ such that $a * a = e$. $\square$

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?

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. □

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 e. First, e is idempotent since $e * e = e$.

Now let $x \in G$ be idempotent, so $x * x = x$. Left-multiply this equation by x' and use associativity:

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

By associativity this is $(x' * x) * x = x' * x$, i.e. $e * x = e$. Hence $x = e$.

Therefore, the only idempotent in G is the identity e. □

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 $x \in G$, it follows that every element is its own inverse; i.e. $x' = x$ for every $x \in G$.

Consider $(a * b) * (a * b)$. By the 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 $n = 1$, we have $(a * b)^1 = a * b$, and 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

$$\begin{aligned}
(a * b)^{k+1} &= (a * b)^k * (a * b) \\
&= ((a^k) * (b^k)) * (a * b) && \text{(inductive hyp.)} \\
&= (a^k * a) * (b^k * b) \\
&= a^{k+1} * b^{k+1}.
\end{aligned}$$

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

$$\begin{aligned}
a' * (a * b) &= a' * (b * a') \\
(a' * a) * b &= a' * b * a' \\
b &= a' * b * a'.
\end{aligned}$$

Multiplying both sides on the right by a, we have $b * a = (a' * b * a') * a$. Since $a' * a = e$, this simplifies to $b * a = a' * b$. Therefore, $b * a = a' * b$. ☐

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 $0 \leq i < j \leq m$ 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 $a^n = e$. ☐