Homework 2 Solutions

Enrique Treviño

September 23, 2014

1 Chapter 3

Problem 1. (**Exercise 2**)
Which of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ form a group? Support your answer in each case.

(a)

$$\begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & a & c & d & a \\ b & b & b & c & d \\ c & c & d & a & b \\ d & d & a & b & c \end{array}$$

(b)

$$\begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & a & b & c & d \\ b & b & a & d & c \\ c & c & d & a & b \\ d & d & c & b & a \end{array}$$

(c)

$$\begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & a & b & c & d \\ b & b & c & d & a \\ c & c & d & a & b \\ d & d & a & b & c \end{array}$$

(d)

$$\begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & a & b & c & d \\ b & b & a & c & d \\ c & c & b & a & d \\ d & d & d & b & c \end{array}$$

Solution 1. To turn in.

Problem 2. (**Exercise 5**)
Describe the symmetries of a square and prove that the set of symmetries is a group. Give a Cayley table for the symmetries. How many ways can the vertices of a square be permuted? Is each permutation necessarily a symmetry of the square? The symmetry group of the square is denoted by D_4.

Solution 2. There are eight symmetries:

1. The identity which we will call id.

2. Reflecting with respect to a vertical line, μ_1.

3. Reflecting with respect to a horizontal line, μ_2.
4. Reflecting with respect to the diagonal BD, μ_3.
5. Reflecting with respect to the diagonal AC, μ_4.
6. Rotating 90 degrees counter-clockwise: ρ_1.
7. Rotating 180 degrees counter-clockwise: ρ_2.
8. Rotating 270 degrees counter-clockwise: ρ_3.

The result of composing one symmetry with another can be seen in the following table:

$\circ$	id	μ_1	μ_2	μ_3	μ_4	ρ_1	ρ_2	ρ_3
id	id	μ_1	μ_2	μ_3	μ_4	ρ_1	ρ_2	ρ_3
μ_1	μ_1	id	ρ_2	ρ_1	ρ_3	μ_3	μ_2	μ_3
μ_2	μ_2	ρ_2	id	ρ_3	ρ_1	μ_4	μ_1	μ_3
μ_3	μ_3	ρ_3	ρ_1	id	ρ_2	μ_2	μ_4	μ_1
μ_4	μ_4	ρ_1	ρ_3	ρ_2	id	μ_1	μ_3	μ_2
ρ_1	ρ_1	μ_4	μ_3	μ_1	μ_2	ρ_2	ρ_3	id
ρ_2	ρ_2	μ_2	μ_1	μ_4	μ_3	ρ_3	id	ρ_1
ρ_3	ρ_3	μ_3	μ_4	μ_2	μ_1	id	ρ_1	ρ_2

Not all permutations of $ABCD$ result in a symmetry. For example the permutation $BACD$, i.e., changing A for B and keeping C and D fixed is not a symmetry since the angle $\angle CAB$ changes from $90°$ to $45°$ with that permutation.

Problem 3. (**Exercise 7**)
Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group.

Solution 3. First let's show that $*$ is closed, i.e., that if $a, b \in S$, then $a * b \in S$. Since S is every real except -1 then we want to show that if $a \neq -1$ and $b \neq -1$, then $a * b \neq -1$. For the sake of contradiction, suppose $a * b = -1$. Then

$$\begin{aligned} a + b + ab &= -1 \\ a(b+1) + b &= -1 \\ a(b+1) &= -(b+1). \end{aligned}$$

Since $b \neq -1$, then we can divide both sides by $b+1$. But then we have that $a = -1$, which contradicts that $a \neq -1$. Therefore $a * b \neq -1$, so $a * b \in S$, so $*$ is a binary operation on S.

Now let's show that $*$ is associative. Suppose $a, b, c \in S$.

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

Therefore $*$ is associative.

Let's show that 0 is the identity for S. Let $a \in S$. Then $a * 0 = a + 0 + 0 = a$ and $0 * a = 0 + 0 + a = a$. Therefore $0 * a = a * 0 = a$, so 0 is the identity of S.

To finish our proof that S is a group, we need to show every element has an inverse. Let $a \in S$. We want to find an inverse for a, so we want to find a $b \neq -1$ such that $a * b = 0$.

$$\begin{aligned} a * b &= 0 \\ ab + a + b &= 0 \\ b(a+1) &= -a \\ b &= -\frac{a}{a+1}. \end{aligned}$$

Since $a \neq -1$, b exists and $a * b = 0$, so $b = -\dfrac{a}{a+1}$ is the inverse of a. Note that $b = -1 + \dfrac{1}{a+1} \neq -1$, so $b \in S$.

We've shown that S is a group together with the operation $*$. To show that it is an abelian group we must prove that $*$ is commutative. Let $a, b \in S$. Then

$$a * b = ab + a + b = ba + b + a = b * a,$$

therefore it is an abelian group.

Problem 4. (**Exercise 14**)
Given the groups $\mathbb{R}^*$ and $\mathbb{Z}$, let $G = \mathbb{R}^* \times \mathbb{Z}$. Define a binary operation $\circ$ on G by $(a, m) \circ (b, n) = (ab, m+n)$. Show that G is a group under this operation.

Solution 4. To turn in.

Problem 5. (**Exercise 16**)
Give a specific example of some group G and elements $g, h \in G$ where $(gh)^n \neq g^n h^n$.

Solution 5. Consider the group D_4 (from Exercise 5). Let $g = \mu_1$ and $h = \mu_3$ and let $n = 2$. Then

$$(gh)^2 = (\mu_1 \circ \mu_3)^2 = (\rho_1)^2 = \rho_2,$$

while

$$g^2 h^2 = (\mu_1^2) \circ (\mu_3^2) = id \circ id = id.$$

Since $\rho_2 \neq id$, then $(gh)^2 \neq g^n h^n$.

Problem 6. (**Exercise 17**)
Give an example of three different groups with eight elements. Why are the groups different?

Solution 6. The groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ have 8 elements. Let's show they are all different. To show their difference we'll look at the subgroups they have.

$\mathbb{Z}_8$ has only one subgroup with 2 elements, namely $\{0, 4\}$, while $\mathbb{Z}_4 \times \mathbb{Z}_2$ has 3 subgroups with 2 elements: $\{(0,0),(2,0)\}$, $\{(0,0),(0,1)\}$, and $\{(0,0),(2,1)\}$. On the other hand, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 7 subgroups with 2 elements: $\{(0,0,0),(1,0,0)\}$, $\{(0,0,0),(1,0,1)\}$, $\{(0,0,0),(1,1,0)\}$, $\{(0,0,0),(1,1,1)\}$, $\{(0,0,0),(0,1,0)\}$, $\{(0,0,0),(0,1,1)\}$, $\{(0,0,0),(0,0,1)\}$. Since all three groups have a different set of subgroups of order 2, they can't be the same group.

Problem 7. (**Exercise 24**)
Let a and b be elements in a group G. Prove that $ab^n a^{-1} = (aba^{-1})^n$ for $n \in \mathbb{Z}$.

Solution 7. For $n = 0$, $ab^0 a^{-1} = aa^{-1} = e$ and $(aba^{-1})^0 = e$ too, so they match. Let's prove it by induction for $n \in \mathbb{N}$. If $n = 1$, then clearly $ab^1 a^{-1} = (aba^{-1})^1$. Suppose that for some $k \geq 1$, then $ab^k a^{-1} = (aba^{-1})^k$. Let's prove that $ab^{k+1} a^{-1} = (aba^{-1})^{k+1}$.

Since $(aba^{-1})^k = ab^k a^{-1}$, then

$$\begin{aligned} (aba^{-1})^{k+1} = (aba^{-1})^k (aba^{-1}) &= ab^k a^{-1} (aba^{-1}) \\ &= ab^k (a^{-1} a) ba^{-1} \\ &= ab^k ba^{-1} \\ &= ab^{k+1} a^{-1}. \end{aligned}$$

Therefore the statement is true for all $n \in \mathbb{N}$. We're left with trying to prove the statement for $n < 0$.

Suppose $n = -m$ where $m \in \mathbb{N}$. We want to show $ab^{-m}a^{-1} = (aba^{-1})^{-m}$. Now, $(aba^{-1})^{-1} = (ab^{-1}a^{-1})$, so $(aba^{-1})^{-m} = (ab^{-1}a^{-1})^{m}$. But since $m \in \mathbb{N}$, then $(ab^{-1}a^{-1})^{m} = ab^{-m}a^{-1}$. Therefore

$$(aba^{-1})^{-m} = ab^{-m}a^{-1}.$$

So the statement is true for negative numbers as well. Now we've shown it for all $n \in \mathbb{Z}$.

Problem 8. (**Exercise 25**)
Let $U(n)$ be the group of units in $\mathbb{Z}_n$. If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$.

Solution 8. $\gcd(n, n-1) = 1$, therefore $n - 1 \in U(n)$. $(n-1)^2 \equiv (-1)^2 \equiv 1 \bmod n$. Since $n > 2$, then $n - 1 > 1$, so $n - 1 \neq 1$. Therefore $k = n - 1$ satisfies the conditions in the problem.

Problem 9. (**Exercise 30**)
Show that if $a^2 = e$ for all elements a in a group G, then G must be abelian.

Solution 9. To turn in.

Problem 10. (**Exercise 33**)
Find all the subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$. Use this information to show that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not the same group as $\mathbb{Z}_9$.

Solution 10. To turn in.

Problem 11. (**Exercise 34**)
Find all the subgroups of the symmetry group of an equilateral triangle.

Solution 11. Define id, ρ_1, ρ_2, μ_1, μ_2, and μ_3 as the 6 symmetries of an equilateral triangle. id is the identity symmetry, ρ_1 is rotating $120°$, ρ_2 is rotating $240°$ and μ_1, μ_2, μ_3 are the three possible reflections. Then the subgroups are:

- $\{id\}$,
- $\{id, \mu_1\}$,
- $\{id, \mu_2\}$,
- $\{id, \mu_3\}$,
- $\{id, \rho_1, \rho_2\}$,
- $\{id, \mu_1, \mu_2, \mu_3, \rho_1, \rho_2\}$.

It is not hard to see that there are no other subgroups. Indeed any subgroup must have id. If you have ρ_1, then you must have ρ_2 and viceversa since $\rho_1 \circ \rho_1 = \rho_2$ and $\rho_2 \circ \rho_2 = \rho_1$. If you have μ_i and ρ_j in the subgroup, then you must have the whole group because $\rho_1\mu_i \neq \rho_2\mu_i$, $\rho_1\mu_i \neq \mu_i$, $\rho_2\mu_i \neq \mu_i$ and neither of them is the identity. So you have at least 6 distinct elements: $\mu_i, \rho_1\mu_i, \rho_2\mu_i, id, \mu_i, \rho_1, \rho_2$. But the whole group of symmetries consists of 6 elements. That means the only subgroups are the subgroups listed.

Problem 12. (**Exercise 36**)
Let $H = \{2^k : k \in \mathbb{Z}\}$. Show that H is a subgroup of $\mathbb{Q}^*$.

Solution 12. To turn in.

Problem 13. (**Exercise 37**)
Let $n = 0, 1, 2, \ldots$ and $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Prove that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. Show that these subgroups are the only subgroups of $\mathbb{Z}$.

Solution 13. First let's show $n\mathbb{Z}$ is a subgroup for any $n \in \mathbb{N} \cup \{0\}$:

(a) First let's show addition is closed on $n\mathbb{Z}$. If $a, b \in n\mathbb{Z}$, then there exist $k_1, k_2 \in \mathbb{Z}$ such that $a = k_1 n$ and $b = k_2 n$. Then
$$a + b = k_1 n + k_2 n = (k_1 + k_2)n \in n\mathbb{Z}.$$

(b) The identity of $\mathbb{Z}$, 0, is an element of $n\mathbb{Z}$, since $0 = n \times 0$, so $0 \in n\mathbb{Z}$.

(c) Finally, let's show that any element of $n\mathbb{Z}$ has an inverse. Indeed if $a \in n\mathbb{Z}$, then $a = k_1 n$ for some integer k_1. Then $-a = -k_1 n = (-k_1)n \in n\mathbb{Z}$. Therefore the inverse of a is also an element of $n\mathbb{Z}$.

By (a), (b) and (c), $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ with the addition operation.

Now, we want to show that all subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ with $n \in \mathbb{N} \cup \{0\}$. Suppose $H \subseteq \mathbb{Z}$ is a subgroup. If $H = \{0\}$, then $H = 0\mathbb{Z}$. Suppose $H \neq \}0\}$. By the Well-Ordering principle, there exists a nonzero element $n \in H$ such that $|n|$ is minimal. Since H is a subgroup of $\mathbb{Z}$, then the inverse of n is also in H, i.e., $-n \in H$. Since n and $-n$, then we can assume without loss of generality that n is positive. Since H is a subgroup, then all multiples of n must be in H. This means that $n\mathbb{Z} \subseteq H$. Now suppose that there is an element $m \in H$ such that $m \notin n\mathbb{Z}$. By the division algorithm, there exist integers q and r such that:
$$m = qn + r,$$
where $0 \leq r < n$. Since $m \notin n\mathbb{Z}$, then $r \neq 0$. Since $m \in H$ and $qn \in H$, then $-qn \in H$, so $m - qn \in H$. Therefore $r \in H$. But $0 < r < n$ which implies that $|r| < |N|$, which contradicts the minimality of $|n|$. This means no element m exists. That proves that $H = n\mathbb{Z}$.

Problem 14. (**Exercise 40**)
Prove that
$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are not both zero}\}$$
is a subgroup of $\mathbb{R}^*$ under the group operation of multiplication.

Solution 14. To turn in.