Worksheet 2: Solutions to selected problems

The best way to understand an abstract definition is to use it. So try it out in the following problems.

1. Which of the following sets are groups with the given binary operation? To show something is a group, you must check that all three axioms are satisfied. To show something is not a group, you must give an example of one axiom failing.

   (a) $(\{1\}, \times)$

Solution. This is a group. It is closed under multiplication and we know multiplication is associative. There is only one element, and $1 \times 1 = 1$, so 1 is the identity element, and 1 is its own inverse. Hence, all axioms are satisfied.

   (b) $(\{1, -1\}, \times)$

Solution. This is a group. It is closed under multiplication because $1 \times 1 = -1 \times -1 = 1$ and $1 \times -1 = -1 \times 1 = 1$ and we know multiplication is associative. 1 is the identity element and the inverse of -1 is itself.

   (c) $(\mathbb{Z}_n, +_n)$

Solution. This is a group. Addition is associative, 0 is the identity, and given any $a \in \mathbb{Z}_n$, the element $n - a \in \mathbb{Z}_n$ satisfies $a +_n (n - a) = 0$ and $(n - a) +_n a = 0$.

   (d) $(\mathbb{Q}, \times)$

Solution. This is not a group. The identity element is 1 but 0 has no inverse.

   (e) $(\mathbb{Q}^\times, \times)$

Solution. This is a group. Multiplication is associative, 1 is the identity, and the inverse of r is $1/r$.

   (f) $(S = \{a + bi \in \mathbb{C} \mid a^2 + b^2 = 1\}, \cdot)$ (feel free to skip if you haven't seen complex numbers before)

Solution. This is a group. Multiplication is always associative, but we must first check that this is closed under multiplication: i.e. if we take two complex numbers $a + bi$ and $c + di$ such that $a^2 + b^2 = 1$ and $c^2 + d^2 = 1$, then the product also satifies that condition. To do this, we simply check:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

and

$$\begin{aligned}(ac - bd)^2 + (ad + bc)^2 &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) = a^2 + b^2 = 1.\end{aligned}$$

The identity element is $1 + 0i = 1$, and to show it is a group, we just need to find the inverse of each element. But a computation shows that $(a + bi)(a - bi) = 1$, so the inverse of each element is $a - bi$ which satisfies $a^2 + (-b^2) = 1$.

   (g) $(S = \{2^n \mid n \in \mathbb{Z}\}, \times)$

Solution. This is a group. Multiplication is associative and $2^n 2^m = 2^{n+m}$ so the set is closed under multiplication. The identity element is $2^0 = 1$ and the inverse of 2^n is 2^{-n}.

(h) $(S = \{A \in M_n(\mathbb{R}) | \det A \neq 0\}, \cdot)$

Solution. This is a group. Multiplication is associative and the set is closed under multiplication because, if A and B are matrices such that $\det A \neq 0$ and $\det B \neq 0$, then $\det(AB) = \det A \det B \neq 0$. The identity element is I_n and, because $\det A \neq 0$ for every matrix in the set, every matrix is invertible.

(i) $(S = \{r \in \mathbb{R} | r \neq -1\}, \star)$ where $a \star b = a + b + ab$

Solution. This is a group. We first check that it is closed under the operation: we need to check that if $a, b \neq -1$, then $a \star b \neq -1$. To do this, assume $a, b \neq -1$ but $a \star b = -1$. Then, $a + b + ab = -1$. With some algebra, this becomes $a(1 + b) = -1 - b$. Because $b \neq -1$, we can divide by $1 + b$ to get $a = (-1 - b)/(1 + b) = -1$, a contradiction. Next, we need to check that the operation is associative:

$$a \star (b \star c) = a \star (b + c + bc) = a + b + c + bc + a(b + c + bc) = a + b + c + ab + ac + bc + abc$$

and

$$(a \star b) \star c = (a + b + ab) \star c = a + b + ab + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc.$$

These agree, so $\star$ is associative. This has an identity element 0 because, for any a, $a \star 0 = a + 0 + 0 = a$ and $0 \star a = 0 + a + 0 = a$. Finally, we need to show that a has an inverse, so there is some element b such that $a \star b = 0$. We simply solve $a + b + ab = 0$ and find that $b = -a/(1 + a)$ is the inverse of a.

2. We observed that, for the symmetries of the triangle, in each row and column of the table representing the binary operation, each group element appeared exactly once. Prove that this is always true, for any group.

Solution. Assume that an element $c \in G$ appears twice in one row. Suppose that row corresponds to the element a. This means that $a \star b_1 = c$ and $a \star b_2 = c$ for group elements $b_1 \neq b_2$. However, using the cancellation law (multiplying both sides on the left by a'), we see that this implies $b_1 = b_2$, a contradiction. Similarly, assume that an element $c \in G$ appears twice in one column and that column corresponds to the element b. This means that $a_1 \star b = c$ and $a_2 \star b = c$ for $a_1 \neq a_2$. Again using the cancellation law (multiplying both sides on the right by b', we see that this implies $a_1 = a_2$, a contradiction. Hence, each element appears exactly one time in any row or column.

3. Assume that ϕ is an isomorphism between binary structures $(S, \star)$ and $(S', \star')$ such that e is an identity element for S. Prove that $\phi(e)$ is an identity element for S'.

Solution. We must show that, for any $s' \in S'$, $s' \star' \phi(e) = \phi(e) \star s' = s'$. Because ϕ is surjective, there is an element s such that $\phi(s) = s'$. Because e is the identity for S, $s \star e = e \star s = s$. Applying ϕ to this equation, we get $\phi(s \star e) = \phi(e \star s) = \phi(s)$, but the homomorphism property implies that $\phi(s) \star' \phi(e) = \phi(e) \star' \phi(s) = \phi(s)$, and $\phi(s) = s'$, so we have shown that $s' \star' \phi(e) = \phi(e) \star' s' = s'$.

4. Assume that ϕ is an isomorphism between groups $(G_1, \star_1)$ and $(G_2, \star_2)$. Prove that ϕ takes inverses to inverses, i.e. $\phi(a') = \phi(a)'$.

Solution. Assume that a' is the inverse of $a \in G_1$. Let e_1 and e_2 denote the identity elements in G_1 and G_2, respectively. We must show that $\phi(a) \star_2 \phi(a') = e_2$ and $\phi(a') \star_2 \phi(a) = e_2$. We do this using the homomorphism property: we know that a' is the inverse of a, so $a \star_1 a' = a' \star_1 a = e_1$. Applying the isomorphism ϕ, we know from Problem 3 that $\phi(e_1) = e_2$, so this implies that

$$\phi(a \star_1 a') = \phi(a' \star_1 a) = e_2$$

and using the homomorphism property, we get the desired result

$$\phi(a) \star_2 \phi(a') = \phi(a') \star_2 \phi(a) = e_2.$$

Therefore, $\phi(a')$ is the inverse of $\phi(a)$.

Here are some harder problems, if you have finished already.

5. For what values of n is $(\mathbb{Z}_n^\times, \cdot_n)$ a group?

Solution. Without proof, I will tell you that the answer is: this is a group if and only if n is 1 or any prime number.

6. First, a definition:

   Definition 0.1. The **order** or **size** of a group G, denoted by $|G|$, is the number of elements in G. The **order** of an element $g \in G$ is the minimal positive integer n such that $g^n = e$.

   If n is a prime number, what is the order of all elements of $(\mathbb{Z}_n, +_n)$?

Solution. If $m = 0$, the order is 1. If m is a nonzero integer in $\mathbb{Z}_n$, the order (under addition) should be the minimal $k > 0$ such that $km \equiv 0 \mod n$. This is the minimal k such that km is divisible by n. If n is prime, it has no factors other than 1 and n, hence km is divisible by n if and only if k or m is divisible by n. Since $m < n$, we must have k divisible by n, and hence the order (the minimal such k) is n.

7. Find two non-isomorphic groups of order 4. Prove that they are not isomorphic. (Symmetries could be a good thing to think about!)

Solution. One group is $(\mathbb{Z}_4, +_4)$: this has order four. Another group G_{rect} could be the symmetries of a non-square rectangle: there are four elements, E, R, F, FR (where R indicates rotating 180 degrees and F is flipping across the vertical axis). These are two groups of order four, but I claim they are not isomorphic. If they were isomorphic, the orders of elements in $\mathbb{Z}_4$ would have to be the same as the orders of the elements in G. But, the orders of the elements in $\mathbb{Z}_4$ are $1, 4, 2, 4$ and the orders of the elements in G_{rect} are $1, 2, 2, 2$.

8. Fix an integer $n > 0$. Define the group $(C_n, \star)$ to be the set $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$ and define $\star$ to be $a^k \star a^j = a^{k+j}$ subject to the rule $a^n = e$. Prove that this is a group. Is it isomorphic to any of the groups that we have already seen?

Solution. Multiplication is associative, e is the identity, and given any element a^k, a^{n-k} is its inverse, so this is a group. It is isomorphic to $(\mathbb{Z}_n, +_n)$. Can you prove this?

9. Is $(C_6, \star)$ isomorphic to $(D_3, \circ)$? (Remember, D_3 was the group of symmetries of the triangle.)

Solution. No, because $(C_6, \star)$ is abelian but $(D_3, \circ)$ is not.