Abstract Algebra
Day 8 Class Work Solutions

1. Come up with as many examples of groups as possible. Be sure to...
   - Specify both the set (e.g., S_3) and the operation (e.g., $\circ$).
   - Check the group properties 1 through 4.
   - Determine if the group is commutative or non-commutative.

   Solution. Answers will vary. Here are some examples:
   - D_4 (symmetries of a square) under composition; non-commutative; see Section 5.2 in the textbook for the verification of its group properties.
   - $\mathbb{Z}$ (integers) under addition; commutative.
   - $\mathbb{Z}_{35}$ under addition; commutative; see Example 8.3 in the textbook.
   - U_{35} under multiplication; commutative; see Example 8.6 in the textbook.

2. Here are some examples of groups under *addition*: $\mathbb{Z}$, $\mathbb{Z}_{10}$, $\mathbb{Z}_7$. Each of these sets is also closed under multiplication. Are they *groups* under multiplication? Why or why not?

   Ans: No. (Why not?)

   Solution. No, they are *not* groups under multiplication. Each of these sets is closed under multiplication, which is an associative operation. Furthermore, each of these sets contain the multiplicative identity 1. However, the zero element $0 \in \mathbb{Z}$ does not have a multiplicative inverse in $\mathbb{Z}$, i.e., there is no integer m such that $0 \cdot m = 1$ and $m \cdot 0 = 1$. The same can be said about $\mathbb{Z}_{10}$ and $\mathbb{Z}_7$.

3. Recall that $U_{10} = \{a \in \mathbb{Z}_{10} \mid a \text{ has a } \textit{multiplicative} \text{ inverse in } \mathbb{Z}_{10}\}$.

   Note: We must be specific about the type of inverse (multiplicative or additive).

   (a) Find the elements of U_{10}. (**Hint:** There are four of them.)

   Solution. $U_{10} = \{1, 3, 7, 9\}$.

   (b) Construct a multiplication table for U_{10}.

   Solution.

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

   (c) Use the table to check the group properties for U_{10}.

   Note: You may simply assume that multiplication is associative.

   Solution.
   1. U_{10} is closed under multiplication. We can see this from the table above, since every entry in the table (i.e., all possible products) is an element of U_{10}.
   2. The associative law holds for multiplication.
   3. U_{10} contains the identity element 1.
   4. Every element in U_{10} has an inverse in U_{10}. Note that 3 and 7 are inverses of each other. Each of 1 and 9 is a self inverse.

   (d) Is U_{10} commutative or non-commutative?

   Solution. U_{10} is commutative. (How can we tell from the table?)

4. With σ, $\tau \in S_3$, we've seen that $(\sigma\tau)^{-1} \neq \sigma^{-1}\tau^{-1}$, but instead $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$.

   (a) Compute $(\sigma\tau)(\tau^{-1}\sigma^{-1})$ and $(\tau^{-1}\sigma^{-1})(\sigma\tau)$.

   Hint: Use the associative law to regroup elements.

   Solution. See the proof in part (b).

   (b) Using your results in part (a), explain why $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$ is *always* true.

   Proof. We will show that $\sigma\tau$ multiplied by $\tau^{-1}\sigma^{-1}$ (on either side) yields the identity element. First, on the right: $(\sigma\tau)(\tau^{-1}\sigma^{-1}) = \sigma(\tau\tau^{-1})\sigma^{-1} = \sigma\,\varepsilon\,\sigma^{-1} = \sigma\sigma^{-1} = \varepsilon$. Here, we used the fact that σ^{-1} and τ^{-1} are inverses of σ and τ, respectively, so that $\sigma\sigma^{-1} = \varepsilon$ and $\tau\tau^{-1} = \varepsilon$. Next, we multiply on the left: $(\tau^{-1}\sigma^{-1})(\sigma\tau) = \tau^{-1}(\sigma^{-1}\sigma)\tau = \tau^{-1}\,\varepsilon\,\tau = \tau^{-1}\tau = \varepsilon$. Thus, the inverse of $\sigma\tau$ is $\tau^{-1}\sigma^{-1}$, which can be written symbolically as $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$. ∎

   (c) Why might this be called the "socks-shoes" property?

   Solution. Think of σ as putting on your socks and τ as putting on your shoes. Then $\sigma\tau$ denotes putting on your socks, followed by your shoes. To undo this process (i.e., $(\sigma\tau)^{-1}$), you must first take off your shoes (i.e., τ^{-1}) and then take off your socks (i.e., σ^{-1}). Therefore, $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$.

5. In S_3, consider again

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

   (a) Elizabeth says, "σ^{-5} is the same as $(\sigma^{-1})^5$." Anita claims that $\sigma^{-5} = (\sigma^5)^{-1}$. With whom do you agree?

   Solution. The two interpretations are equivalent. Applying the socks-shoes property five times (imagine four layers of socks, followed by shoes), we obtain

$$(\sigma^5)^{-1} = (\sigma\sigma\sigma\sigma\sigma)^{-1} = \sigma^{-1}\sigma^{-1}\sigma^{-1}\sigma^{-1}\sigma^{-1} = (\sigma^{-1})^5.$$

   ← Therefore, we can unambiguously say σ^{-5}.

   (b) Compute $(\sigma^{-1})^5$ and $(\sigma^5)^{-1}$, and verify that they're equal.

   Solution. Both $(\sigma^{-1})^5$ and $(\sigma^5)^{-1}$ are equal to σ. (I'll leave the calculations to you!) Note that since $\sigma^3 = \varepsilon$, we have $\sigma^{-5} = \sigma^{-5} \cdot \varepsilon \cdot \varepsilon = \sigma^{-5} \cdot \sigma^3 \cdot \sigma^3 = \sigma$.

6. **Theorem (left cancellation):** Let a, b, c be elements of a group. If $ab = ac$, then $b = c$.

   (a) In $\mathbb{Z}_{10}$, we have $2 \cdot 6 = 2 \cdot 1$, even though $6 \neq 1$. Explain why this does *not* violate the (left) cancellation law.

   Hint: See Problem #2.

   Solution. This does *not* violate the (left) cancellation law, because $\mathbb{Z}_{10}$ is *not* a group under multiplication (it is a group under addition, though).

   (b) Define σ, τ, $\mu \in S_3$, respectively, by

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

   Compute the products $\sigma\tau$ and $\mu\sigma$ and verify that they're equal.

   Solution. Both $\sigma\tau$ and $\mu\sigma$ are equal to

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

   (c) Anita says, "We have $\sigma\tau = \mu\sigma$. If we cancel σ from both sides, we get $\tau = \mu$. How's that possible?" How would you respond to her?

   Solution. The cancellation must occur on the *same* side of each expression. We cannot cancel σ on the *left* of $\sigma\tau$ and on the *right* of $\mu\sigma$.

7. Prove the left cancellation law, stated in Problem #6. In your proof, be sure to specify the group properties that are used.

Note: Right cancellation is defined/proved similarly.

PROOF. Let a, b, c be elements of a group. Assume $ab = ac$. Multiply both sides of the equation *on the left* by a^{-1} to obtain $a^{-1}(ab) = a^{-1}(ac)$. Using the associative law gives $(a^{-1}a)b = (a^{-1}a)c$. Since $a^{-1}a = \varepsilon$, we get $\varepsilon b = \varepsilon c$. Finally, ε keeps all group elements unchanged, i.e., $\varepsilon b = b$ and $\varepsilon c = c$. Thus $b = c$, as desired. ■

8. In Problem #3, we saw that U_{10} is a group under multiplication.

   (a) What about U_{35}? Is it a group under multiplication? How do you know?

   ← Constructing a table is *not* recommended...

   (b) More generally, explain why U_m is a group under multiplication.

Solution. See Example 8.6 in the textbook for an explanation of why U_{35} is a group under multiplication. That explanation can be generalized to U_m as well.

9. (a) Consider $U_8 = \{1, 3, 5, 7\}$. Verify that $a^2 = 1$ for all $a \in U_8$.

   ← U_8 is a group under multiplication.

   (b) Is U_8 commutative or non-commutative?

   (c) Repeat parts (a) and (b) with the group U_{12}. (First find the elements of U_{12}.)

10. Consider the subset $C(h) = \{\varepsilon, r_{180}, h, v\}$ of D_4. In Day 5 Class Work, we verified that $C(h)$ is a group under composition.

   Recall: $C(h)$ is called the *centralizer* of h in D_4.

   (a) Now verify that $\alpha^2 = \varepsilon$ for all $\alpha \in C(h)$.

   (b) Is $C(h)$ commutative or non-commutative?

   Ans: Commutative.

11. (a) **Prove:** Let G be a group. If $g^2 = \varepsilon$ for all $g \in G$, then G is commutative.

   (b) Is the converse of the statement in part (a) true? If it's true, prove it. If it's false, give a counterexample.