Abstract Algebra
Day 16 Class Work Solutions

1. Let g be a group element with $\text{ord}(g) = 6$. Consider the cyclic group $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. We just saw that $\langle g \rangle = \{g^0, g^1, g^2, g^3, g^4, g^5\}$, where $g^0 = \varepsilon$.

   ← i.e., $\langle g \rangle$ is the set of all integer powers of g.

   (a) Write down the distinct elements of the additive group $\mathbb{Z}_6$.

   Solution. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

   (b) How do the elements in $\mathbb{Z}_6$ and $\langle g \rangle$ "match up"?

   Solution. There is a *bijection* function (i.e., one-to-one and onto) $\theta : \mathbb{Z}_6 \to \langle g \rangle$ where $\theta(a) = g^a$ for all $a \in \mathbb{Z}_6$. For example, $\theta(3) = g^3$, so $3 \in \mathbb{Z}_6$ and $g^3 \in \langle g \rangle$ "match up."

   (c) Compute the following and describe how they're related:

   - $3 + 5$ in $\mathbb{Z}_6$ and $g^3 \cdot g^5$ in $\langle g \rangle$.
   - -2 in $\mathbb{Z}_6$ and $(g^2)^{-1}$ in $\langle g \rangle$.

   Solution. See the solution for part (d).

   (d) How do $\mathbb{Z}_6$ and $\langle g \rangle$ behave similarly as groups?

   ← Compare addition in $\mathbb{Z}_6$ & multiplication in $\langle g \rangle$.

   Solution. The operations of $\mathbb{Z}_6$ and $\langle g \rangle$ "match up." Noting that $g^6 = \varepsilon$, we have...

   - $3 + 5 = 2$ in $\mathbb{Z}_6$, which is just like $g^3 \cdot g^5 = g^{3+5} = g^2$ in $\langle g \rangle$.
   - The additive identity of $\mathbb{Z}_6$ is 0, and the multiplicative identity of $\langle g \rangle$ is $g^0 = \varepsilon$.
   - In $\mathbb{Z}_6$, $2 + 4 = 0$ so that the additive inverse of 2 is 4 (i.e., $-2 = 4$). And in $\langle g \rangle$, $g^2 \cdot g^4 = \varepsilon$ so that the multiplicative inverse of g^2 is g^4 (i.e., $(g^2)^{-1} = g^4$).

   Thus, addition $\mathbb{Z}_6$ *feels like* multiplication in $\langle g \rangle$.

2. Let g be a group element with $\text{ord}(g) = 6$. Consider the function $\theta : \mathbb{Z}_6 \to \langle g \rangle$ where $\theta(a) = g^a$ for all $a \in \mathbb{Z}_6$. For example, $\theta(3) = g^3$.

   (a) Make sense of the equation: $\theta(3 + 5) = \theta(3) \cdot \theta(5)$.

   Solution. Using the law of exponents (i.e., $g^{a+b} = g^a \cdot g^b$), we have

   $$\theta(3 + 5) = g^{3+5} = g^3 \cdot g^5 = \theta(3) \cdot \theta(5),$$

   so that $\theta(3 + 5) = \theta(3) * \theta(5)$.

   (b) How does the equation in part (a) capture the notion that the operations of $\mathbb{Z}_6$ and $\langle g \rangle$ "match up"?

   Solution. Given $3, 5 \in \mathbb{Z}_6$, we can...

   - Add them first in $\mathbb{Z}_6$, then apply θ to the sum: $\theta(3 + 5)$.
   - Apply θ to each, then multiply in $\langle g \rangle$: $\theta(3) * \theta(5)$.

   To say that the group operations "match up" means

   $$\theta(3 + 5) = \theta(3) * \theta(5).$$

   Again, addition in $\mathbb{Z}_6$ *feels like* multiplication in $\langle g \rangle$.

3. Let g be a group element with *infinite* order. Consider the function $\theta : \mathbb{Z} \to \langle g \rangle$ where $\theta(a) = g^a$ for all $a \in \mathbb{Z}$.

← Or choose $g = 3$ in the multiplicative group $\mathbb{R}^*$.

   (a) Find $a \in \mathbb{Z}$ such that $\theta(a) = g^{-34}$.

   Solution. $a = -34$.

   (b) Show that θ is onto.

   Proof. Let $y \in \langle g \rangle$ so that $y = g^x$ for some integer x. Then $y = \theta(x)$ where $x \in \mathbb{Z}$. Thus, θ is onto. ■

   (c) Explain why $g^{12} \neq g^7$.

   Hint: Assume $g^{12} = g^7$ and obtain a contradiction.

   Solution. Suppose for contradiction that $g^{12} = g^7$. Multiplying both sides by g^{-7} yields $g^5 = \varepsilon$. But this contradicts the fact that g has infinite order. Thus, $g^{12} \neq g^7$.

   (d) Show that θ is one-to-one.

   Note: Since $\text{ord}(g) = \infty$, there is no positive integer n such that $g^n = \varepsilon$.

   ← In other words, $g^n = \varepsilon$ would imply that $n = 0$.

   Proof. Suppose $\theta(a) = \theta(b)$ where $a, b \in \mathbb{Z}$. Then $g^a = g^b$, and multiplying both sides by g^{-b} yields $g^{a-b} = \varepsilon$. Since $\text{ord}(g) = \infty$, the exponent $a - b$ must equal 0. Thus $a = b$ so that θ is one-to-one. ■

   (e) Show that $\theta(a + b) = \theta(a) \cdot \theta(b)$ for all $a, b \in \mathbb{Z}$.

   Note: Thus, we say that θ is *operation preserving*.

   Solution. Let $a, b \in \mathbb{Z}$. Then $\theta(a + b) = g^{a+b} = g^a * g^b = \theta(a) * \theta(b)$.

4. Let G and H be groups. Consider $\theta : G \to H$ where $\theta(a \cdot b) = \theta(a) \cdot \theta(b)$ for all $a, b \in G$.

   (a) In the equation $\theta(a \cdot b) = \theta(a) \cdot \theta(b)$, there are two products: $a \cdot b$ and $\theta(a) \cdot \theta(b)$. In which group, G or H, does each of these multiplications take place?

   Ans: $a \cdot b$ occurs in G, and $\theta(a) \cdot \theta(b)$ happens in H.

   Solution. $a \cdot b$ occurs in G, and $\theta(a) \cdot \theta(b)$ happens in H.

   (b) Suppose θ is one-to-one. Prove that if H is commutative, then G is commutative.

   (c) Suppose θ is onto. Prove that if G is commutative, then H is commutative.

   Proof. Assume G is commutative. Let $h, k \in H$. We must show that $h \cdot k = k \cdot h$. Since θ is onto, there exist $a, b \in G$ such that $h = \theta(a)$ and $k = \theta(b)$. Therefore, $h \cdot k = \theta(a) \cdot \theta(b) = \theta(a \cdot b)$ and $k \cdot h = \theta(b) \cdot \theta(a) = \theta(b \cdot a)$. Since G is commutative, we have $a \cdot b = b \cdot a$, which implies $\theta(a \cdot b) = \theta(b \cdot a)$ so that $h \cdot k = k \cdot h$. Hence, H is commutative. ■

5. Recall that $\mathbb{R}$ is the additive group of all real numbers. Define $\mathbb{R}^{>0} = \{r \in \mathbb{R} \mid r > 0\}$, i.e., the set of all *positive* real numbers.

   (a) Explain why $\mathbb{R}^{>0}$ is a group under multiplication.

   (b) Define a function $\alpha : \mathbb{R} \to \mathbb{R}^{>0}$ where $\alpha(x) = 3^x$ for all $x \in \mathbb{R}$. Show that α is one-to-one and onto.

   Proof. First, we'll show that α is one-to-one. Assume $\alpha(a) = \alpha(b)$ where $a, b \in \mathbb{R}$. Then $3^a = 3^b$. By taking the log base 3 of both sides of $3^a = 3^b$, we obtain $\log_3 3^a = \log_3 3^b$, which simplifies to $a = b$.

   Next, we'll show that α is onto. Assume $y \in \mathbb{R}^{>0}$. Then let $x = \log_3 y \in \mathbb{R}$ so that $\alpha(x) = 3^x = 3^{\log_3 y} = y$. ■

   (c) Show that $\alpha(x + y) = \alpha(x) \cdot \alpha(y)$ for all $x, y \in \mathbb{R}$.

   Solution. For $x, y \in \mathbb{R}$, we have $\alpha(x + y) = 3^{x+y} = 3^x \cdot 3^y = \alpha(x) \cdot \alpha(y)$.

6. Consider again the additive group $\mathbb{R}$, and also the multiplicative group $\mathbb{R}^*$ of nonzero real numbers. Explain why there cannot be a function $\theta : \mathbb{R} \to \mathbb{R}^*$ that is one-to-one and onto, and satisfies $\theta(x + y) = \theta(x) \cdot \theta(y)$ for all $x, y \in \mathbb{R}$.

   Hint: If such a function exists, then $\theta(r) = -1$ for some $r \in \mathbb{R}$. Explain why that would lead to a contradiction.

7. **(Some Food for Thought)** Let $S = \{a, b, c, d, e\}$ and $T = \{x, y, z\}$.

   (a) How many different *onto* functions are there from S to T?

   (b) What if S and T have m and n elements, respectively?