Abstract Algebra
Day 23 Class Work Solutions

Unless specified otherwise, assume the shortcut holds in G/H. ← i.e., $aH \cdot bH = (ab)H$.

1. G/H is a group. Therefore, any property that we know about groups applies to G/H. Let's consider the "socks-shoes," for example. What goes into the empty boxes?

$$(aH \cdot bH)^{-1} = \square H \cdot \square H.$$

Solution. The "socks-shoes" property says $(\alpha \cdot \beta)^{-1} = \beta^{-1} \cdot \alpha^{-1}$. With $\alpha = aH$ and $\beta = bH$, we have

$$(aH \cdot bH)^{-1} = (bH)^{-1} \cdot (aH)^{-1} = b^{-1}H \cdot a^{-1}H.$$

2. Let G be a commutative group and H its subgroup. Prove that G/H is commutative.

Hint: Start with two elements of G/H. What do those elements look like? **Ans:** aH and bH.

Proof. Let $aH, bH \in G/H$. Then, since $ab = ba$ in G, we have

$$aH \cdot bH = (ab)H = (ba)H = bH \cdot aH.$$

Thus, $aH \cdot bH = bH \cdot aH$ so that G/H is commutative. ■

3. Consider the subgroup $H = \{1, 3, 9\}$ of U_{13}.

   (a) Find the order of 4 in U_{13}. **Ans:** $\text{ord}(4) = 6$.

   Solution. We have $\text{ord}(4) = 6$, because...

$$\begin{aligned} 4^1 &= 4 \\ 4^2 &= 3 \\ 4^3 &= 12 \\ 4^4 &= 9 \\ 4^5 &= 10 \\ 4^6 &= 1 \end{aligned}$$

   (b) Find the order of $4H$ in U_{13}/H.

   Solution. Note that $1H = 3H = 9H$. We have $\text{ord}(4H) = 2$, because...

$$\begin{aligned} (4H)^1 &= 4^1H = 4H \\ (4H)^2 &= 4^2H = 3H = 1H \end{aligned}$$

   (c) Anita claims, "If $\text{ord}(4) = 6$, then $(4H)^6 = 4^6H = 1H$. Thus, $\text{ord}(4H) = 6$, too." Fix the error in her argument.

   Solution. $(4H)^6 = 1H$ implies that the order of $4H$ is a divisor of 6. We saw in part (b) that $\text{ord}(4H) = 2$, which is indeed a divisor of 6.

4. **Prove:** Let $a \in G$ with finite order. Then $\text{ord}(aH)$ in G/H is a divisor of $\text{ord}(a)$ in G. ← Anita's error is quite useful in this proof.

Hint: In a group, say $(\text{blah})^{10}$ equals the identity. What can you say about $\text{ord}(\text{blah})$?

Proof. Let $n = \text{ord}(a)$ so that $a^n = \varepsilon$. Then $(aH)^n = a^nH = \varepsilon H$. Since $(aH)^n = \varepsilon H$, it follows that $\text{ord}(aH)$ is a divisor of n. ■

5. Consider the statement:

   If $aH = bH$ in G/H, then $a = b$ in G.

   Is it true or false? If it's true, prove it. If it's false, give a counter-example.

   Solution. This is false. With $G = U_{13}$ and $H = \{1, 3, 9\}$, we have $1H = 3H$ in U_{13}/H, but $1 \neq 3$ in U_{13}.

6. **Prove:** $(gH)^n = \varepsilon H$ if and only if $g^n \in H$. **Hint:** $aH = H \Leftrightarrow a \in H$.

   Proof. Assume $(gH)^n = \varepsilon H$. We have $g^n H = (gH)^n = \varepsilon H = H$. Thus, $g^n \in H$.

   Next assume $g^n \in H$. Then $g^n H = H$. But since $g^n H = (gH)^n$, we have $(gH)^n = H = \varepsilon H$, as desired. ■

7. Suppose $[G : H] = n$. Show that $g^n \in H$ for all $g \in G$.

   Recall: $[G : H]$ is the number of (left) cosets of H, which is also the size of G/H.

   Hint: Consider the element $gH \in G/H$, and let $d = \text{ord}(gH)$. How are d and n related?

   Proof. Let $g \in G$, and consider $gH \in G/H$. Let d be the order of gH in G/H so that $(gH)^d = \varepsilon H$. Since G/H contains n elements, the order d of gH is a divisor of n. Thus, $n = dk$ for some integer k. We then have

   $$(gH)^n = (gH)^{dk} = ((gH)^d)^k = (\varepsilon H)^k = \varepsilon H.$$

   Thus, $(gH)^n = \varepsilon H$. Then by Problem #6, we conclude that $g^n \in H$. ■

8. Let G be a group and $Z = \{z \in G \mid zg = gz \text{ for all } g \in G\}$. Prove that the shortcut holds in G/Z. In other words, given $aZ, bZ \in G/Z$, define the coset product by ← i.e., Z is the *center* of G.

   $$aZ \cdot bZ = \{\alpha \cdot \beta \mid \alpha \in aZ,\ \beta \in bZ\}.$$

   Then show that $aZ \cdot bZ = (ab)Z$.

   Note: This is a set equality proof. You must show $aZ \cdot bZ \subseteq (ab)Z$ and $(ab)Z \subseteq aZ \cdot bZ$.

   Solution. This is similar to Day 22 Class Work, Problem #12, with H replaced by Z. In fact, the proof is nearly identical. The only difference is the reason for the claim

   $$\alpha \cdot \beta = (ah)(bk) = (ab)(hk) \in (ab)Z.$$

   Since $h \in Z$, it commutes with all elements of G. In particular, we have $hb = bh$ so that

   $$\alpha \cdot \beta = (ah)(bk) = a(hb)k = a(bh)k = (ab)(hk) \in (ab)Z.$$

9. Let G be a group and H a subgroup of G. Determine if each statement is true or false. If it's true, prove it. If it's false, give a counterexample.

   (a) If G and H are finite, then G/H is finite.

   (b) If G/H is finite, then G and H are finite.

   (c) If G is infinite and H is finite, then G/H is infinite.

10. (a) Find an additive group G, a subgroup H, and an element $a \in G$ such that:

    $$a + H \neq 0 + H,\ \text{ord}(a + H) \text{ in } G/H \text{ is finite, and ord}(a) \text{ in } G \text{ is infinite.}$$

Solution. $G = \mathbb{Z}$, $H = 5\mathbb{Z}$, $a = 1$. Then, $1 + H \neq 0 + H$, $\text{ord}(1 + H)$ in $\mathbb{Z}/H$ is 5, and $\text{ord}(1)$ in $\mathbb{Z}$ is infinite.

(b) Same as part (a), but this time, find a commutative, multiplicative group.

Solution. $G = \mathbb{R}^*$ (the group of nonzero reals), $H = \mathbb{Q}^*$ (nonzero rationals), $a = \sqrt{3}$. Then $aH \neq 1H$, since $a \notin H$. And $\text{ord}(aH)$ in G/H is 2, but $\text{ord}(a)$ in G is infinite.

11. If G/H has an element of order n, show that G has an element of order n.

← Assume that each $g \in G$ has finite order.

Hint: Let $gH \in G/H$ be an element of order n. Now, come up with an element in G with order n. An earlier problem might come in handy.

12. Let G be a group, and define Z as in Problem #8.

Prove: If G/Z is cyclic, then G is commutative.