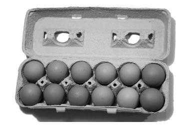
Abstract Algebra
Day 20 Class Work Solutions

1. (a) There are lots of eggs and dozen egg cartons. If all the eggs are in cartons and all the cartons are full, can there be 1000 eggs? Why or why not?

   ← This kind of carton:

   Solution. No, because 12 is *not* a divisor of 1000.

   (b) Let G be a group. If a subgroup H has 12 elements, can the group G contain 1000 elements? Why or why not?

   Solution. No, because 12 is *not* a divisor of 1000.

2. Let H be a subgroup of a *finite* group G. In answering these, try to *justify* your claims.

   (a) Suppose $\#G = 28$ and $\#H = 4$, where $\#G$ and $\#H$ denote the sizes of G and H, respectively. Find $[G : H]$, i.e., the number of distinct left cosets of H.

   Ans: $[G : H] = 7$.

   Solution. All cosets of H have 4 elements, just like H. And given that the cosets of H form a *partition* of G (i.e., they cover all of G without any overlap), there must be $28 \div 4 = 7$ distinct cosets of H. Therefore, $[G : H] = 7$.

   (b) Can a group with 28 elements have a subgroup of size 5? Why or why not? Give an explanation using cosets.

   Solution. No, because 5 is *not* a divisor of 28. See part (d) below for an explanation.

   (c) Find a general formula for $[G : H]$. Explain your reasoning.

   Solution. $[G : H] = \frac{\#G}{\#H}$, where $\#G$ and $\#H$ refer to the size of G and H (i.e., the number of elements), respectively.

   (d) Explain why $\#H$ is a divisor of $\#G$.

   Solution. Since all cosets of H have the same size, namely $\#H$, and the distinct cosets of H form a partition of G (i.e., they fill up G without any overlap), it follows that $\#H$ is a divisor of $\#G$. See Section 20.2 in the textbook for more details.

3. Let G be a finite group, and consider an element $g \in G$ with $\text{ord}(g) = 6$.

   (a) Let $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ be the cyclic subgroup generated by g. Write down the *distinct* elements of $\langle g \rangle$. How many elements does $\langle g \rangle$ contain?

   Solution. By Theorem 13.17, $\langle g \rangle$ contains 6 distinct elements, namely

   $$\langle g \rangle = \{\varepsilon,\, g^1,\, g^2,\, g^3,\, g^4,\, g^5\}.$$

   (b) Can the group G contain 34 elements? Why or why not?

   Ans: No. (Why not?)

   Hint: Apply Problem #2(d) with $H = \langle g \rangle$.

   Solution. No. With $H = \langle g \rangle$, we have $\#H = 6$. Based on Problem #2(d), we conclude that $\#G$ must be a multiple of 6. In particular, we have $\#G \neq 34$.

4. **Prove:** Let G be a finite group and $g \in G$. Then $\text{ord}(g)$ is a divisor of $\#G$.

   Hint: See Problem #3.

   Proof. Let $n = \text{ord}(g)$. Then the cyclic subgroup $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ contains n distinct elements, namely $\langle g \rangle = \{\varepsilon,\, g^1,\, g^2,\, g^3,\, \ldots,\, g^{n-1}\}$. Since $\langle g \rangle$ is a subgroup of G, we conclude that $\#\langle g \rangle$ is a divisor of $\#G$. Thus, $n = \text{ord}(g)$ is a divisor of $\#G$. ■

5. Suppose a group G contains 5 elements, and let $g \in G$ be a non-identity element.

   (a) Find $\text{ord}(g)$.

   Ans: $\text{ord}(g) = 5$.

(b) How many elements does the cyclic subgroup $\langle g \rangle$ contain?

(c) Explain why G is cyclic with generator g.

Solution. By the theorem in Problem #4, $\text{ord}(g)$ is a divisor of $\#G = 5$. Since 5 is prime, its only positive divisors are 1 and 5. And since $g \neq \varepsilon$, we know that $\text{ord}(g) \neq 1$. Thus we must have $\text{ord}(g) = 5$, which implies that the cyclic subgroup $\langle g \rangle$ contains 5 elements, namely $\langle g \rangle = \{\varepsilon, g^1, g^2, g^3, g^4\}$. Since G also has 5 elements, we have $G = \langle g \rangle$, so that G is cyclic with generator g.

6. Repeat Problem #5 with a group G that contains 7 elements; 19 elements; 101 elements; p elements where p is prime.

Solution. Our work in Problem #5 can be generalized by replacing 5 with any prime p. Then we obtain the following conclusion:

> Let G be a group with p elements, where p is prime. Then G is cyclic with $G = \langle g \rangle$, where g is any non-identity element of G.

7. Consider the group D_4 and its subgroup $H = \{\varepsilon, r_{180}, d, d'\}$.

Note: You should be able to complete this problem *without* the table for D_4.

(a) Find $[D_4 : H]$. **Ans:** $[D_4 : H] = 2$.

Solution. Since $\#D_4 = 8$ and $\#H = 4$, we have $[D_4 : H] = 8 \div 4 = 2$.

(b) Suppose $a \in H$. Determine the elements in the coset aH.

Solution. Since $a \in H$, we have $aH = H$.

(c) Same as part (b), but with $a \notin H$.

Solution. Since $a \notin H$, we have $aH \neq H$. There are only two cosets, and thus aH must be the other coset. Since the distinct cosets H and aH form a partition of D_4 (i.e., they cover all of D_4 without any overlap), the coset aH must contain the remaining elements of D_4 that are not in H. Therefore, $aH = \{r_{90}, r_{270}, h, v\}$.

8. In this problem, you'll prove that the distinct cosets of H form a *partition* of G, i.e.,

- they cover all of G, and
- they do not overlap with each other.

(a) Give an example that illustrates this notion of a partition.

(b) **Prove:** Every element of G is contained in some coset of H. ← i.e., they cover all of G.

(c) **Prove:** If $aH \neq bH$, then aH and bH do not have any element in common. ← i.e., they don't overlap.

Hint: Think contrapositive.

Solution. See Section 20.2 in the textbook for details.

9. Let G be a group and H and K its subgroups. Define $M = \{g \in G \mid g \in H \text{ and } g \in K\}$. ← i.e., M is the *intersection* of H and K.

(a) **Prove:** M is a subgroup of G.

(b) If $\#H = 21$ and $\#K = 32$, find $\#M$. Explain your reasoning.

Solution. We've seen that M is a subgroup of G. In fact, $M \subseteq H$ and $M \subseteq K$, so that M is a subgroup of H and of K. Thus, $\#M$ is a divisor of both $\#H = 15$ and $\#K = 28$. Since $\gcd(15, 28) = 1$, we must have $\#M = 1$. In other words, $M = \{\varepsilon\}$.

10. Consider the prime number $p = 3$.
    (a) Choose an integer a, compute $a^p - a$, and verify that p is a divisor of $a^p - a$.
    (b) Repeat part (a) with another integer a of your choice.
    (c) Repeat part (a) again, this time with a negative integer a.

11. (a) Repeat Problem #10 with prime $p = 5$; with prime $p = 7$; with prime $p = 11$.
    (b) Repeat Problem #10 with one more prime number of your choice.
    (c) What conjecture do you have?

12. **Prove:** Let p be a prime number. Prove that p is a divisor of $a^p - a$ for all $a \in \mathbb{Z}$.

← This is called *Fermat's little theorem*.