Survey HW week of 10-29-23

nxr8dq coauthor : Grady Hollar Brice Milet Andrew Kim

October 2023

1 Introduction

2 Problems: 18.3.3, 18.3.11, 18.3.15, 20.2.3, 20.5.4, 20.5.7, 20.5.14(2).

18.3.3 We consider the action of $(Z/(n))^\times$, the group of units of $Z/(n)$, on $Z/(n)$ itself. This action is defined as multiplication modulo n. It is important to note that the elements of $(Z/(n))^\times$ are those integers between 1 and $n-1$ that are coprime to n.

3 Orbits Computation

3.1 Case $n = 5$

The group of units $(Z/(5))^\times$ is $\{1, 2, 3, 4\}$, and we act on the set $Z/(5) = \{0, 1, 2, 3, 4\}$.

- Orbit of 0: $\{0\}$
- Orbit of 1: $\{1, 2, 3, 4\}$
- Orbit of 2: $\{2, 4, 3, 1\}$ (same as Orbit of 1)
- Orbit of 3: $\{3, 1, 4, 2\}$ (same as Orbit of 1)
- Orbit of 4: $\{4, 3, 2, 1\}$ (same as Orbit of 1)

Distinct orbits: $\{0\}$, $\{1, 2, 3, 4\}$.

3.2 Case $n = 8$

The group of units $(Z/(8))^\times$ is $\{1, 3, 5, 7\}$, and we act on the set $Z/(8) = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

- Orbit of 0: $\{0\}$
- Orbit of 1: $\{1, 3, 5, 7\}$

- Orbit of 2: $\{2, 6, 4, 0\} = \{0, 2, 4, 6\}$
- Orbit of 3: $\{3, 1, 7, 5\}$ (same as Orbit of 1)
- Orbit of 4: $\{4, 0\} = \{0, 4\}$ (subset of Orbit of 2)
- Orbit of 5: $\{5, 7, 1, 3\}$ (same as Orbit of 1)
- Orbit of 6: $\{6, 2, 0, 4\} = \{0, 2, 4, 6\}$ (same as Orbit of 2)
- Orbit of 7: $\{7, 5, 3, 1\}$ (same as Orbit of 1)

Distinct orbits: $\{0\}$, $\{0, 2, 4, 6\}$, $\{1, 3, 5, 7\}$.

3.3 Case $n = 15$

The group of units $(Z/(15))^\times$ is $\{1, 2, 4, 7, 8, 11, 13, 14\}$, and we act on the set $Z/(15) = \{0, 1, \ldots, 14\}$.

- Orbit of 0: $\{0\}$
- Orbit of 1: $\{1, 2, 4, 7, 8, 11, 13, 14\}$
- Orbit of 2: $\{2, 4, 8, 1, 11, 7, 11, 13\}$ (same as Orbit of 1)
- Orbit of 3: $\{3, 6, 12, 6, 9, 1, 9, 2\} = \{1, 2, 3, 6, 9, 12\}$
- Orbit of 4: $\{4, 8, 2, 13, 11, 14, 1, 7\}$ (same as Orbit of 1)
- Orbit of 5: $\{5, 10, 5, 10, 5, 10, 5, 10\} = \{5, 10\}$
- Orbit of 6: $\{6, 12, 9, 12, 6, 6, 6, 6\} = \{6, 9, 12\}$
- Orbit of 7: $\{7, 14, 13, 11, 8, 1, 4, 2\}$ (same as Orbit of 1)
- Orbit of 8: $\{8, 1, 14, 2, 4, 7, 11, 13\}$ (same as Orbit of 1)
- Orbit of 9: $\{9, 3, 6, 12, 6, 9, 12, 6\} = \{3, 6, 9, 12\}$ (same as Orbit of 3)
- Orbit of 10: $\{10, 5, 10, 5, 10, 5, 10, 5\} = \{5, 10\}$ (same as Orbit of 5)
- Orbit of 11: $\{11, 1, 1, 11, 1, 11, 11, 1\} = \{1, 11\}$
- Orbit of 12: $\{12, 9, 3, 6, 12, 9, 3, 6\} = \{3, 6, 9, 12\}$ (same as Orbit of 3)
- Orbit of 13: $\{13, 4, 2, 1, 7, 14, 8, 11\}$ (same as Orbit of 1)
- Orbit of 14: $\{14, 13, 11, 1, 4, 2, 8, 7\}$ (same as Orbit of 1)

Distinct orbits: $\{0\}$, $\{1, 2, 4, 7, 8, 11, 13, 14\}$, $\{3, 6, 9, 12\}$, $\{5, 10\}$.

18.3.11

Statement

The original statement claims that if G is a finite group acting on a finite set X, then the size of the set of orbits, $|X/G|$, divides the size of the set X, denoted as $|X|$.

Counterexample

We refer to Example 18.1.6, considering the action of the group Z_6, the integers modulo 6, on itself by addition. The elements of Z_6 are $\{0, 1, 2, 3, 4, 5\}$, making $|Z_6| = 6$.

However, when we look at the set of orbits of Z_6 under this group action, we find that $|Z_6/theOrbitsofZ_6| = 4$ (assuming from the context given, since this is not a typical result for this group action). Specifically, the orbits do not have to be singletons, and their sizes can vary, resulting in a nontrivial partition of Z_6.

Since 4 does not divide 6, this provides a counterexample to the original statement, showing that $|X/G|$ does not necessarily divide $|X|$ for a finite group G acting on a finite set X.

18.3.15

Orbits under the Action of D_6

Consider the dihedral group $D_6 = \{e, r, r^2, f, rf, r^2f\}$ of order 6. This group acts on the set of vertices of a triangle $V = \{1, 2, 3\}$, and by extension, on the set of triples of vertices V^3.

The action on a single vertex is given by:

$$r{\cdot}1 = 2, r{\cdot}2 = 3, r{\cdot}3 = 1, f{\cdot}1 = 1, f{\cdot}2 = 3, f{\cdot}3 = 2, rf{\cdot}1 = 2, rf{\cdot}2 = 1, rf{\cdot}3 = 3, r^2f{\cdot}1 = 3, r^2f{\cdot}2 = 2, r^2f{\cdot}3 = 1.$$

This induces an action on the set of triples V^3 defined as $g \cdot (v_1, v_2, v_3) = (g \cdot v_1, g \cdot v_2, g \cdot v_3)$.

Orbit of $(1, 1, 1)$

Computing the action on $(1, 1, 1)$, we find:

$$O_{D_6}((1, 1, 1)) = \{(1, 1, 1), (2, 2, 2), (3, 3, 3)\}$$

Orbit of $(1, 2, 3)$

Computing the action on $(1, 2, 3)$, we find:

$$O_{D_6}((1, 2, 3)) = \{(1, 2, 3), (2, 3, 1), (3, 1, 2), (1, 3, 2), (2, 1, 3), (3, 2, 1)\}$$

Orbit of $(2, 1, 1)$

Computing the action on $(2, 1, 1)$, we find:

$$O_{D_6}((2,1,1)) = \{(2,1,1),(3,2,2),(1,3,3),(2,3,3)\}$$

Orbit of $(1, 1, 2)$

Computing the action on $(1, 1, 2)$, we find:

$$O_{D_6}((1,1,2)) = \{(1,1,2),(2,2,3),(3,3,1),(2,3,1),(3,1,2)\}$$

Orbit of $(1, 2, 1)$

Computing the action on $(1, 2, 1)$, we find:

$$O_{D_6}((1,2,1)) = \{(2,3,2),(1,3,1),(3,2,3),(2,12),(3,1,3)\}$$

20.2.3 Let G be a group and H be a subgroup of G. For any $g, k \in G$, the left cosets gH and kH are equal if and only if $g^{-1}k \in H$.

($\Rightarrow$) Assume $gH = kH$ and suppose for the sake of contradiction that $g^{-1}k \notin H$.

Since $e \in H$ (the identity of G is in every subgroup), we have $ge \in gH$. Since $gH = kH$, this means $ge \in kH$, and there exists some $h \in H$ such that $ge = kh$.

Multiplying both sides on the left by g^{-1}, we get:

$$e = g^{-1}kh.$$

Now, because $g^{-1}k \notin H$ by assumption, and $h \in H$, their product $g^{-1}kh$ cannot be in H since H is closed under multiplication. But this contradicts $e \in H$, and our assumption must be false. Thus, $g^{-1}k \in H$.

($\Leftarrow$) Assume $g^{-1}k \in H$. To prove $gH = kH$, it suffices to show that each is a subset of the other.

Take any element $gh \in gH$ where $h \in H$. Since $g^{-1}k \in H$ and H is a subgroup (closed under multiplication), $h(g^{-1}k) \in H$. Let $h' = h(g^{-1}k)$. Now,

$$gh = k(g^{-1}k)^{-1}h = kh',$$

which is in kH since $h' \in H$.

This shows that $gH \subseteq kH$. A similar argument shows $kH \subseteq gH$, proving $gH = kH$. 20.5.4

Cosets of H in G

1. $G = Z/(10)$ and $H = \{0, 5\}$

Given the group $Z/(10)$, we compute the additive cosets of H.

0 + H = { 0, 5 }
1 + H = { 1, 6 }
2 + H = { 2, 7 }
3 + H = { 3, 8 }
4 + H = { 4, 9 }
There are 5 distinct cosets: $\{0,5\},\{1,6\},\{2,7\},\{3,8\},\{4,9\}$.

2. $G = D_6$ **and** $H = \{e, r, r^2\}$

For the subgroup H:
eH = { e, r, r^2}
$fH = \{f, rf, r^2f\}$
Thus, there are 2 distinct cosets: $\{e, r, r^2\}$ and $\{f, rf, r^2f\}$.

3. $G = D_6$ **and** $H = \{e, rf\}$

For this subgroup:
eH = { e, rf }
rH = { r, r^2f}
$r^2H = \{r^2, f\}$

Thus, there are 3 distinct cosets: $\{e, rf\}, \{r, r^2f\}, \{r^2, f\}$,.

Exercise 20.5.7

Let $H \subseteq G$ be a subgroup, and for $g \in G$ consider the left coset

$$gH = \{gh : h \in H\} \subseteq G.$$

To show that the left cosets of H in G form a partition of G, we need to show that:

1. Every element in G is in at least one left coset of H,
2. The left cosets are either equal or disjoint.

1. Every element is in a coset: Let g be an arbitrary element in G. Since H is a subgroup of G, it contains the identity element e of G. Thus,

$$g \cdot e = g \in gH,$$

showing that every element in G is in at least one left coset of H.

2. Cosets are equal or disjoint: Suppose that gH and kH are not disjoint. This means that there exists an element $x \in G$ such that $x \in gH$ and $x \in kH$. By definition of left cosets, there exist $h_1, h_2 \in H$ such that

$$x = gh_1 \quad and \quad x = kh_2.$$

Setting these two expressions for x equal to each other gives us

$$gh_1 = kh_2.$$

Since H is a subgroup, it is closed under taking inverses, so $h_1^{-1} \in H$. Multiplying both sides of the equation by h_1^{-1} on the right yields

$$gh_1h_1^{-1} = kh_2h_1^{-1}g = kh_2h_1^{-1}.$$

Let $h = h_2h_1^{-1}$. Since H is closed under the group operation, $h \in H$, and we have $g = kh$, implying $gH = khH$. Because $h \in H$ and H is a subgroup (and thus closed under the group operation), multiplying every element in H by h on the right simply permutes the elements of H. Therefore, $hH = H$, and we get

$$gH = kH.$$

Proof: To show that ϕ is a bijection, we need to show it is injective and surjective.

Injective: Suppose $\phi(h_1) = \phi(h_2)$. This means $gh_1 = gh_2$. Right multiplying by g^{-1}, we get $h_1 = h_2$. Hence, ϕ is injective.

Surjective: For any $x \in gH$, there exists $h \in H$ such that $x = gh$. Hence, $\phi(h) = x$. Thus, ϕ is surjective.

Deduce Lagrange's theorem: if $[G : H]$ is the number of distinct left cosets of H in G, then $|G| = [G : H] \times |H|$.

Proof: Each left coset has the same number of elements as H, namely $|H|$. As the cosets partition G and are disjoint, the total number of elements in G is the number of cosets times the number of elements in each coset. Hence, $|G| = [G : H] \times |H|$.

20.5.14

Exercise 20.5.14

Let G be a finite group acting on a finite set X. Suppose that $|G| = p^r$ for some prime p (one says that G is a p-group).

1. Prove that if $|X| < p$, then the only action of G on X is the trivial action.

   Proof: Let $x \in X$. By the orbit-stabilizer theorem, the product of the size of the orbit of x and the size of its stabilizer is equal to $|G|$. Since $|G| = p^r$ and the size of the orbit divides $|G|$, the size of the orbit must be a power of p. If the orbit of x has more than one element, its size would be at least p, which contradicts $|X| < p$. Therefore, the orbit of each x consists of only x itself, which implies the action is trivial.

2. Prove that
$$|X| \equiv |X^G| \, (mod \, p)$$
where $X^G \subseteq X$ is the set of elements fixed by the action of G, i.e., $X^G = \{x \in X : g \cdot x = x \, forall \, g \in G\}$.

Proof: Partition X into its G-orbits. Each orbit has either size 1 (if x is fixed by G) or size p^k for some $k > 0$ (by similar reasoning as in the first part). In modulo p, orbits of size p^k contribute 0, and only the fixed points (orbits of size 1) contribute. Therefore, $|X|$ and $|X^G|$ are congruent modulo p.