Abstract Algebra I

Homework 5

B13902024 張沂魁
Due: 15th October 2025

1. Let G be a finite group that acts on a finite set S. We (again) define the orbit of $s \in S$ to be

$$O(s) = \{g \cdot s : g \in G\},$$

and the stabilizer of s in G to be

$$G_s = \{g \in G : g \cdot s = s\}.$$

(a) Check that for any two distinct elements $s, t \in S$, we either have $O(s) = O(t)$ or $O(s) \cap O(t) = \varnothing$.

(b) Verify that G_s is a subgroup of G, and that the map given by

$$\{\text{cosets of } G_s \text{ in } G\} \to O(s), \quad gG_s \mapsto g \cdot s$$

is a well-defined bijection.

(c) Conclude that $|G_s| \cdot |O(s)| = |G|$. (This is called the **orbit-stabilizer theorem**.)

Solution:

(a) For $s, t \in S$ with $s \neq t$, if $O(s) \cap O(t) = \varnothing$, then it is the second case. If $p \in O(s) \cap O(t)$, then $p = g_1 s = g_2 t$ for some $g_1, g_2 \in G$. Hence, we know

$$s = \left(g_1^{-1} g_2\right) t \in O(t),$$

and thus $O(s) \subseteq O(t)$. Similarly, we know $O(t) \subseteq O(s)$, and thus $O(s) = O(t)$.

(b) We first check that G_s is a subgroup of G. Since G acts on S, so $e \cdot s = s$, and thus $e \in G_s$, which means G_s is non-empty. Also, if $g_1, g_2 \in G_s$, then $g_1 s = g_2 s = s$, so

$$(g_1 g_2)\, s = g_1\,(g_2 s) = g_1 s = s,$$

which means $g_1 g_2 \in G_s$. Besides, if $gs = s$, then $s = g^{-1} g s = g^{-1}(gs) = g^{-1} s$, so $g^{-1} \in G_s$. By above arguments, G_s is a subgroup of G.

Now we show that the map given by

$$\Phi : \{\text{cosets of } G_s \text{ in } G\} \to O(s), \quad gG_s \mapsto g \cdot s$$

is well-defined. If $g_1 G_s = g_2 G_s$, then since $e \in G_s$, so $g_1 \in g_2 G_s$, so $g_1 = g_2 g_3$ for some $g_3 \in G_s$, which means $g_3 s = s$. Thus,

$$g_1 s = g_2 g_3 s = g_2 s,$$

so the map Φ is well-defined.

Next, we show that Φ is a bijection. If $g_1 s = g_2 s$, then $g_2^{-1} g_1 s = s$, so $g_2^{-1} g_1 \in G_s$, and thus

$$g_1 = g_2\left(g_2^{-1} g_1\right) \in g_2 G_s.$$

Hence, $g_1 = g_2 g$ for some $g \in G_s$, and for all $g' \in G_s$ we have $g_1 g' = g_2 g g'$. Now we claim that $gg' \in G_s$. Since

$$gg's = gs = s,$$

so we proved it. By this, we know $g_1 g' = g_2 g g' \in G_s$, which means $g_1 G_s \subseteq g_2 G_s$. Now since we also have $g_1^{-1} g_2 s = s$, so we can similrly derive $g_2 G_s \subseteq g_1 G_s$, and thus $g_1 G_s = g_2 G_s$, which means Φ is injective. Now we show that Φ is surjective. For all $p \in O(s)$, we know $p = g \cdot s$ for some $g \in G$, so $\Phi(g) = g \cdot s = p$, which means Φ is surjective, and thus Φ is bijective.

(c) By (b), we know $[G : G_s] = |O(s)|$, and since $[G : G_s] \cdot |G_s| = |G|$, so we have

$$|G_s| \cdot |O(s)| = |G|.$$

2. Consider the action of G on itself given by $(g, h) \mapsto g^{-1}hg$, called **conjugation**. In this case the orbit of $h \in G$ is called the **conjugacy class** of h and we denote it by

$$\text{class}(h) = \{g^{-1}hg : g \in G\},$$

and the stabilizer is called the **centralizer** of h and is denoted by

$$C_G(h) = \{g \in G : g^{-1}hg = h\}.$$

Elements in the same conjugacy class are called **conjugates** of one another.

(a) Let $\text{class}(h_1), \ldots, \text{class}(h_n)$ be the distinct conjugacy classes of G, i.e.

$$\bigcup_{i=1}^{n} \text{class}(h_i) = G.$$

Derive the **class equation**

$$|G| = \sum_{i=1}^{n} \frac{|G|}{|C_G(h_i)|}.$$

(b) Furthermore, suppose for each $i = m+1, \ldots, n$, we have $|\text{class}(h_i)| = 1$, while for $i = 1, \ldots, m$, we have $|\text{class}(h_i)| > 1$. Show that

$$|G| = |Z(G)| + \sum_{i=1}^{m} \frac{|G|}{|C_G(h_i)|},$$

where $Z(G)$ denotes the **center** of G. (Usually the class equation is written in this second form.)

(c) Let p be a prime, and $n \geq 1$. If $|G| = p^n$, deduce that $Z(G) \neq \{e\}$.

Solution:

(a) We first show that for $i \neq j$, we must have $\text{class}(h_i) \cap \text{class}(h_j) = \varnothing$. If $p \in \text{class}(h_i) \cap \text{class}(h_j)$, then $p = g_1^{-1} h_i g_1 = g_2^{-1} h_j g_2$, so $g_2 g_1^{-1} h_1 g_1 g_2^{-1} = h_j$, and thus for all $q \in \text{class}(h_j)$, we know

$$q = g_3^{-1} h_j g_3 = g_3^{-1} g_2 g_1^{-1} h_i g_1 g_2^{-1} g_3 \in \text{class}(h_i),$$

which shows $\text{class}(h_j) \subseteq \text{class}(h_i)$. Similarly, we can show that $\text{class}(h_i) \subseteq \text{class}(h_j)$, and thus $\text{class}(h_i) = \text{class}(h_j)$, which is a contradiction since $\text{class}(h_i)$ and $\text{class}(h_j)$ are distinct conjugacy classes of G. Hence, we know

$$|G| = \sum_{i=1}^{n} |\text{class}(h_i)|.$$

Now we show that $|\text{class}(h_i)| = \frac{|G|}{|C_G(h_i)|}$ for all $1 \leq i \leq n$. Suppose $G = \left\{\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_{|G|}\right\}$, then we can collect

$$\mathcal{G}_1^{-1} h_i \mathcal{G}_1,\ \mathcal{G}_2^{-1} h_i \mathcal{G}_2,\ \ldots,\ \mathcal{G}_{|G|}^{-1} h_i \mathcal{G}_{|G|},$$

we know these are all the elements in class(h_i) but contains repeated elements, and we have collected $|G|$ things, and we called this collection $\mathcal{C}$. Now we claim that for every $p \in \mathcal{C}$, p is counted $|C_G(h_i)|$ times, and thus $|\text{class}(h_i)| = \frac{|G|}{|C_G(h_i)|}$. If $p \in \mathcal{C}$, then $p = g_1^{-1} h_i g_1$ for some $g_1 \in G$, and we know for all $g_2 \in C_G(h_i)$,

$$g_1^{-1} g_2^{-1} h_i g_2 g_1 = g_1^{-1} h_i g_1 = p,$$

and note that for all distinct $u, v \in C_G(h_i)$, $ug_1 \neq vg_1$, so in $\mathcal{C}$ we counted p at least $|C_G(h_i)|$ times. Now if we count p in $\mathcal{C}$ more than $|C_G(h_i)|$ times, then we know

$$p = g_k^{-1} h_i g_k \text{ with } g_k \in G \quad \forall 1 \leq k \leq |C_G(h_i)| + 1,$$

where $g_j \neq g_k$ for all $1 \leq j < k \leq |C_G(h_i)| + 1$. Hence, we have

$$g_1^{-1} h_i g_1 = g_k^{-1} h_i g_k \iff g_k g_1^{-1} h_i g_1 g_k^{-1} = h_i$$

for all $1 \leq k \leq |C_G(h_i)| + 1$. Hence, $g_1 g_k^{-1} \in C_G(h_i)$. Note that for distinct l, m, $g_1 g_l^{-1} \neq g_1 g_m^{-1}$, so $C_G(h_i)$ contains at least $|C_G(h_i)| + 1$ elements, which is a contradiction, and we're done. Hence, we have shown that $|\text{class}(h_i)| = \frac{|G|}{|C_G(h_i)|}$, and thus

$$|G| = \sum_{i=1}^{n} |\text{class}(h_i)| = \sum_{i=1}^{n} \frac{|G|}{|C_G(h_i)|}.$$

(b) Note that

$$Z(G) = \{g \in G : gx = xg \quad \forall x \in G\}.$$

Suppose $S = \bigcup_{i=m+1}^{n} \text{class}(h_i)$, we will show that $|Z(G)| = |S|$. For $n \geq i \geq m+1$, since $|\text{class}(h_i)| = 1$, so we know $\frac{|G|}{|C_G(h_i)|} = 1$, and this gives $|G| = |C_G(h_i)|$, which means for all $g \in G$, we have $g^{-1} h_i g = h_i$, which gives $h_i \in Z(G)$. Also, since $h_i = e^{-1} h_i e \in \text{class}(h_i)$, so class$(h_i) = \{h_i\}$ since $|\text{class}(h_i)| = 1$. Hence, we have

$$S = \bigcup_{i=m+1}^{n} \text{class}(h_i) = \{h_{m+1}, h_{m+2}, \ldots, h_n\} \subseteq Z(G).$$

Now if $g' \in Z(G)$, then we know $g'x = xg'$ for all $x \in G$. Also, we know $g' \in \text{class}(h_i)$ for some i and this i is unique. Hence, $g' = g^{-1} h_i g$ for some $g \in G$. Now since $g'g = gg'$, which gives $g^{-1} g' g = g'$, so we have $g^{-1} g' g = g' = g^{-1} h_i g$, so we have $g' = h_i$. Now since

$$u^{-1} h_i u = u^{-1} g' u = g' \quad \forall u \in G,$$

so class$(h_i) = \{h_i\}$, which means $g' \in S$. Hence, we have $Z(G) \subseteq S$, and thus $|Z(G)| = |S|$. Hence,

$$|G| = |S| + \sum_{i=1}^{m} \frac{|G|}{|C_G(h_i)|} = |Z(G)| + \sum_{i=1}^{m} \frac{|G|}{|C_G(h_i)|}.$$

(c) Suppose by contradiction, $Z(G) = \{e\}$, then we know

$$p^n - 1 = |G| - 1 = \sum_{i=1}^{m} \frac{|G|}{|C_G(h_i)|}$$

by (b), and since $|\text{class}(h_i)| = \frac{|G|}{|C_G(h_i)|} > 1$ for all $1 \leq i \leq m$, so

$$p \mid \frac{|G|}{|C_G(h_i)|} = \frac{p^n}{|C_G(h_i)|} \quad \forall 1 \leq i \leq m,$$

and thus

$$p \mid \sum_{i=1}^{m} \frac{|G|}{|C_G(h_i)|} = p^n - 1,$$

which is a contradiction. Hence, $Z(G) \neq \{e\}$.

3. The rest of the homework has nothing to do with group actions.

   Let G be a finite group and H a subgroup. The **index** of H in G, denoted $[G : H]$, is the quantity $|G|/|H|$. For another subgroup $K \leq G$, we are interested in questions about $HK = \{hk : h \in H, k \in K\}$ or KH.

   (a) Prove that
   $$|HK| = \frac{|H||K|}{|H \cap K|}.$$

   (b) Prove that
   $$[G : H \cap K] \leq [G : H][G : K],$$
   with equality if and only if $G = HK$.

   (c) Prove that HK is a subgroup of G if and only if $HK = KH$.

   (d) Prove that if $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.

   (In general, $[G : H]$ is defined to be the number of distinct left cosets of H in G, since our current definition does not make sense if G is infinite. Then the problem of interest would be when H is a subgroup of finite index, but we do not go into that here.)

   Solution:

   (a) Suppose $H = \left\{\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_{|H|}\right\}$ and $K = \left\{\mathcal{K}_1\mathcal{K}_2, \ldots, \mathcal{K}_{|K|}\right\}$, then we can collect all $\mathcal{H}_i\mathcal{K}_j$ with $1 \leq i \leq |H|$ and $1 \leq j \leq |K|$, then there are $|H||K|$ things in this collection, and we know we have counted all things of HK but we have counted some repeated things. Now we claim that each element in HK is counted exactly $|H \cap K|$ times. Suppose $h_1k_1 \in HK$ with $h_1 \in H$ and $k_1 \in K$, then for all $p \in H \cap K$, we know
   $$h_1k_1 = h_1p^{-1}pk_1 = \left(ph_1^{-1}\right)^{-1}(pk_1),$$
   and $\left(ph_1^{-1}\right)^{-1} \in H$ and $pk_1 \in K$. Note that for all $q \neq p$ and $q \in H \cap K$, $qk_1 \neq pk_1$, so $\left(ph_1^{-1}\right)^{-1}(pk_1)$ and $\left(qh_1^{-1}\right)^{-1}(pk_1)$ are both counted in the previously mentioned collection. Hence, h_1k_1 is counted at least $|H \cap K|$ times in the collection. Now if h_1k_1 is counted more than $|H \cap K|$ times, then
   $$h_1k_1 = h_mk_m \text{ with } h_m \in H, k_m \in K \quad \forall 1 \leq m \leq |H \cap K| + 1,$$
   and $h_i \neq h_j$ and $k_i \neq k_j$ for any distinct i, j. Hence, we know
   $$h_m^{-1}h_1 = k_mk_1^{-1} \in H \cap K \quad \forall 1 \leq m \leq |H \cap K| + 1.$$
   Note that $h_i^{-1}h_1 \neq h_j^{-1}h_1$ for all $i \neq j$. This means $H \cap K$ has at least $|H \cap K| + 1$ elements, which is a contradiction. Hence, each h_1k_1 is counted exactly $|H \cap K|$ times in the collection, and thus
   $$|HK| = \frac{|H||K|}{|H \cap K|}.$$

(b) Note that

$$\frac{[G:H][G:K]}{[G:H\cap K]} = \frac{\frac{|G|^2}{|H||K|}}{\frac{|G|}{|H\cap K|}} = \frac{|G|}{\frac{|H||K|}{|H\cap K|}} = \frac{|G|}{|HK|},$$

and since $HK \subseteq G$, so $\frac{|G|}{|HK|} \geq 1$, and the equality holds if and only if $G = HK$, and thus

$$[G:H][G:K] \geq [G:H\cap K]$$

with equality if and only if $G = HK$.

(c)

($\implies$) If HK is a subgroup of G, then for all $p \in KH$, we know $p = kh$ with $k \in K$ and $h \in H$, ans thus $h^{-1}k^{-1} \in HK$, and since HK is a group, so

$$p = kh = \left(h^{-1}k^{-1}\right)^{-1} \in HK,$$

so $KH \subseteq HK$. Also, we know

$$|HK| = \frac{|H||K|}{|H\cap K|} = |KH|,$$

so we have $HK = KH$.

($\impliedby$) If $HK = KH$, then since $e \in H$ and $e \in G$, so $e = e \cdot e \in HK$, so HK is non-empty, and suppose $h_1k_1, h_2k_2 \in HK$ with $h_1, h_2 \in H$ and $k_1, k_2 \in K$, and also we know $k_1h_2 = h_3k_3$ for some $h_3 \in H$ and $k_3 \in K$, so

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1h_3k_3k_2 \in HK.$$

Now if $h_1k_1 \in HK$ for $h_1 \in H$ and $k_1 \in K$, then

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK.$$

Thus, HK is a subgroup of G since $HK \subseteq G$.

(d) By (b) we know $[G:H\cap K] \leq [G:H][G:K]$, and since $H\cap K$ is a subgroup of G, so we have

$$[G:H\cap K] = [G:H][H:H\cap K]$$
$$[G:H\cap K] = [G:K][K:H\cap K].$$

Hence, $[G:H] \mid [G:H\cap K]$ and $[G:K] \mid [G:H\cap K]$, and since $[G:H]$ and $[G:K]$ are relatively prime, so we have

$$[G:H][G:K] \mid [G:H\cap K],$$

so $[G:H][G:K] \leq [G:H\cap K]$, and thus we have

$$[G:H][G:K] \leq [G:H\cap K] \leq [G:H][G:K],$$

so $[G:H\cap K] = [G:H][G:K]$, and by (b) we know this means $G = HK$.

4. Let G be an abelian group of order $2n$. If n is odd, prove that there is only one element of order 2.

Solution: Suppose $g \neq h$ with $g, h \in G$ has $o(g) = o(h) = 2$, then we know $g^2 = h^2 = e$, so we know $S = \{e, g, h, gh\}$ is a subgroup of G since $(gh)^2 = ghgh = g^2h^2 = e$ and we can easily check S satisfies all the other group conditions. Hence, $|G| = [G:S]|S|$, and thus

$$4 = |S| \mid |G| = 2(2k+1) = 4k+2,$$

which is impossible.