Abstract algebra I Homework 5

B13902022 賴昱錡

1)

(a)

Suppose that for any two distinct elements $s, t \in S$, we have $O(s) \neq O(t)$ and $O(s) \cap O(t) \neq \emptyset$. There exists $g_1, g_2 \in G$ such that $g_1 s = g_2 t \Rightarrow t = g_2^{-1} g_1 s$, hence, for every $g \in G$, we have $gt = g g_2^{-1} g_1 s \in O(s)$, i.e., there's always one corresponding element in $O(s)$ for every element in $O(t)$, similarity we have $gs = g g_1^{-1} g_2 t \in O(t)$, so $O(s) = O(t)$, which contradicts our assumption. Thus $O(s) \neq O(t)$ **and** $O(s) \cap O(t) \neq \emptyset$ can't be true at the same time, we either have $O(s) = O(t)$ or $O(s) \cap O(t) = \emptyset$.

(b)

e, the identity element of G, is in G_s trivially, also for any $u, v \in G_s$, $(uv)s = us = s \Rightarrow (uv) \in G_s$, also $us = s, s = u^{-1}s \Rightarrow u^{-1} \in G_s$, thus G_s is closed under taking products and inverses, $G_s \leq G$.

Let the map be ϕ and $g_1, g_2 \in G$, if $g_1 G_s = g_2 G_s$ and $g_1, g_2 \in G$, then $g_2^{-1} g_1 G_s = G_s \Rightarrow g_2^{-1} g_1 \in G_s$. Hence, $g_2^{-1} g_1 s = s, g_1 s = g_2 s$, from $\phi(g_1 G_s) = \phi(g_2 G_s)$ we know ϕ is well-defined.

To prove the injectivity of ϕ, if $g_1 s = g_2 s$ $(g_1, g_2 \in G)$, then $g_1^{-1} g_2 s = s \Rightarrow g^{-1} g_2 \in G_s$, so $g^{-1} g_2 G_s = G_s$, we have $g_1 G_s = g_2 G_s$.

For every $u \in O(s)$, it can be written as the form: $u = gs$ for some $g \in G$, so $u = \phi(gG_s)$. ϕ is surjective. Since ϕ is both injective and surjective, ϕ is a well-defined bijection.

(c)

By the result in (b), we know $|G : G_s| = |G|/|G_s| = |O(s)|$, hence $|G_s||O(s)| = |G|$.

2)

(a)

If G is a finite group, then for any element $a \in G$, the element of class(a) and the left cosets of centralizer $C_G(a)$ form a bijection. Since for any two elements $u = b^{-1}, v = c^{-1}$ $(b, c$ are the inverse of u, v in G) belonging to the same coset (so $u = vz, c = zb$ for some $z \in C_G(a)$) give the same element when conjugating a: (since z commutes with a)

$$u^{-1}au = bab^{-1} = (cz^{-1})a(cz^{-1})^{-1} = cz^{-1}azc^{-1} = cz^{-1}zac^{-1} = cac^{-1} = v^{-1}av$$

also, every cosets can be written as the form $gC_G(a)$ for some $g \in G$, it must can be mapped from $g^{-1}ag$, hence, there's one-to-one correspondence between conjugacy class of a and the cosets of $C_G(a)$, so the size of conjugacy class a is equal to $[G : C_G(a)]$. (btw, $C_G(a)$ is trivially a subgroup of G, since it contains identity, also suppose $x, y \in C_G(a)$, then $(xy)^{-1}axy = a, xax^{-1} = a$, it's closed under group operations and taking inverse.)

Thus, the number of elements in conjugacy class of a is the index $[G : C_G(a)]$ of the centralizer $C_G(a)$ in G, also the given conjugacy classes are disjoint, so $|G| = \sum_{i=1}^{n}[G : C_G(h_i)] = \sum_{i=1}^{n} \frac{|G|}{|C_G(h_i)|}$.

(b)

Observe that each of the elements in $Z(G)$ will forms a conjugacy class containing only itself, this is trivial by definition, if $z \in Z(G)$, then $g^{-1}zg = zg^{-1}g = z \forall g \in G$, so:

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

(c)

Since the size of any conjugacy class divides the $|G|$ (because $|\mathrm{class(h_i)}| = \frac{|G|}{|C_G(h_i)|}$), so the sizes of them are some power of p, hence, $|G| = |Z(G)| + \sum_{i=1}^{m} p^{k_i}$, where $0 < k_i < n$. From this we found that p must divides $|Z(G)|$, so $|Z(G)| > 1$.

3)

(a)

Note that HK is the union of left cosets of K, namely, $HK = \bigcup_{h \in H} hK$. Suppose $h_1K = h_2K$, then $h_2^{-1}h_1K = K \Rightarrow h_2^{-1}h_1 \in K \Rightarrow h_2^{-1}h_1 \in H \cap K$. $H \cap K$ is trivially a subgroup of H, since for any $u, v \in H \cap K$, then $uv \in H$ and $uv \in K$, $u^{-1} \in H$ and $u^{-1} \in K$, we have $uv, u^{-1} \in H \cap K$, also $H \cap K$ contains the identity, thus $H \cap K \leq H$.

Since $h_2^{-1}h_1 \in H \cap K$ implies $h_1(H \cap K) = h_2(H \cap K)$, the number of left cosets of K equals to the left cosets of $H \cap K$ in H. By Lagrange's Theorem, the number is $\frac{|H|}{|H \cap K|}$, also each left cosets of K have the size of $|K|$. Hence, $|HK| = \frac{|H||K|}{|H \cap K|}$.

(b)

To prove the inequality, it sufficies to show that the map:

$$G/(H \cap K) \to G/H \times G/K \text{ given by } g(H \cap K) \mapsto (gH, gK)$$

is well-defined and injective, since the injectivity implies the size of $G/(H \cap K)$ is less than or equal to the size of $G/H \times G/K$, which is $|G : H||G : K|$. Suppose $g_1(H \cap K) = g_2(H \cap K)$ $(g_1, g_2 \in G)$, then $g_2^{-1}g_1(H \cap K) = (H \cap K)$ implies $g_2^{-1}g_1 \in (H \cap K)$. So $g_2^{-1}g_1H = H \Rightarrow g_1H = g_2H$ and $g_2^{-1}g_1K = K \Rightarrow g_1K = g_2K$, we have $(g_1H, g_1K) = (g_2H, g_2K)$, hence the map is well defined.

Let $(g_1H, g_1K) = (g_2H, g_2K)$ for some $g_1, g_2 \in G$, then we have $g_2^{-1}g_1 \in (H \cap K)$ from $g_2^{-1}g_1H = H$ and $g_2^{-1}g_1K = K$, thus, $g_2^{-1}g_1(H \cap K) = (H \cap K) \Rightarrow g_1(H \cap K) = g_2(H \cap K)$, so the map is injective. As a result, the inequality $|G : (H \cap K)| \leq |G : H||G : K|$ holds.

If $G = HK$, then $|G| = |HK| = \frac{|H||K|}{|H \cap K|}$ by (a). We obtain that $[G : H \cap K] = \frac{|H||K|}{|H \cap K|^2}$ and $[G : H][G : K] = \frac{|G|^2}{|K||H|} = \frac{|H||K|}{|H \cap K|^2}$. Thus, $[G : H \cap K] = [G : H][G : K]$. On the other hand, if $[G : H \cap K] = [G : H][G : K]$, then $|G| = \frac{|H||K|}{|H \cap K|}$. Since $|HK| = \frac{|H||K|}{|H \cap K|} = |G|$ and HK is a subset of G, we must have $G = HK$.

(c)

If $HK = KH$, every element hk in HK can be written as $k'h'$, for every $h, k \in HK$, for some $k' \in K, h' \in H$. Clearly, HK contains e, the identity element in G. Suppose $u, v \in HK = KH$, $u = h_1k_1, v = k_2h_2$, then $uv = h_1k_1k_2h_2$ $(h_1, h_2 \in H$ and $k_1, k_2 \in K)$, let $k_1k_2 = k_3 \in K$, then $uv = h_1k_3h_2 = h_1hk = h'k \in HK$ for some $h, h' \in H, k \in K, hk = k_3h_2, h' = h_1h$, thus HK is closed under taking products. Also, $u^{-1} = k_1^{-1}h_1^{-1}$ and every element in KH must can be written as ab for some $, a \in H, b \in K$, since $k^{-1} \in K, h^{-1} \in H$, so $u^{-1} \in HK$, HK is closed under taking inverse. In conclusion, $HK \leq G$ if $HK = KH$.

Conversely, if $HK \leq G$. Obviously, $K \in HK$ and $H \in HK$, by the closure property of subgroups (because $HK \leq G$), $KH \subseteq HK$. For any $hk \in HK, h \in H, k \in K$, since HK is a subgroup of G, let $a = h_1k_1, h_1 \in H, k_1 \in H$ be its inverse in HK, then $hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$, we conclude that KH contains HK. Since HK and KH contains each other, we have $HK = KH$. So HK is a subgroup of G if and only if $HK = KH$.

(d)

Since $H \cap K$ itself is a group (Let $x, y \in H \cap K$, then $xy \in H$ and $xy \in K$ and $x^{-1} \in H$ and $x^{-1} \in K$, so $xy \in H \cap K$ and $x^{-1} \in H \cap K$, here proves its closure), we have $(H \cap K) \leq H$ and $(H \cap K) \leq K$, also:

$$[G : H \cap K] = [G : H][H : (H \cap K)]$$
$$[G : H \cap K] = [G : K][K : (H \cap K)]$$

so $[G : H \cap K]$ is divided by both $[G : H]$ and $[G : K]$, by (b) and proposition above we conclude that:

$$\operatorname{lcm}([G : H], [G : K]) \leq [G : H \cap K] \leq [G : H][G : K]$$

Since $[G : H], [G : K]$ are coprime, $\operatorname{lcm}([G : H], [G : K]) = [G : H][G : K]$, we obtain $[G : H \cap K] = [G : H][G : K]$, by (b), the equality implies $G = HK$.

4)

Theorem: (Cauchy's Theorem) Let G be a finite group and p be a prime. If p divides the order of G, then G has an element of order p.

Proof. We first prove the case when G is abelian, and then the general case, both proof uses strong induction on $n = |G|$. When $n = p$, all non-identity elements have order of p by Lagrange's theorem. Suppose G is abelian first, take any non-identity element a, let H be the cyclic group it generates, if p divides $|H|$, then $a^{|H|/p}$ is an element with order p. If p doesn't divide $|H|$, then it divides $[G : H]$, the order of the quotient group G/H (It's a group since every subgroup of abelian group is normal), which contains and element of order p by the inductive hypothesis. Suppose the element is xH for some x in G, if the order of x in G is m, then $x^m = e$ in G gives $(xH)^m = H$, so p divides m, $x^{m/p}$ is an element of order p in G, completing the proof for abelian case.

In the general case, when $n = p$, all non-identity elements have order of p by Lagrange's theorem, this is the base case. Let Z be the center of G, which is a abelian subgroup of G, if p divides $|Z|$, then by the result of abelian case, Z contains at least one element of order p. If p doesn't divide $|Z|$, by the class equation proved in problem 2:

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

there exists one conjugacy class of non-central element a whose size is not divisible by p, its size is $[G : C_G(a)]$, but G is divisible by p, so p must divides the order of the subgroup $C_G(a)$, the group contains an element with order p by inductive hypothesis, and we are done. $\square$

By Cauchy's theorem, since $p = 2$ divides $|G|$, there exists at least one element of order 2.

Suppose $u, w \in G, u \neq v, u \neq e, v \neq e$ have order 2, then the subgroup generated by u, w is $\{e, u, w, uw\}$, where e is the identity element of G. All the elements are unique since if $uw = e$, u or w would have two inverses, also $uw = u$ or $uw = w$ implies $w = e$ or $w = e$, both cases create condradiction. These four elements are the all of it and form a group since G is abelian and it's closed under taking any products or inverses:

$$
\begin{aligned}
u^2 &= e \\
w^2 &= e \\
uw &= uw \\
wu &= uw \\
(uw)u = u^2w &= w \\
(uw)w = uw^2 &= u \\
u(uw) &= w \\
w(uw) &= u \\
(uw)(uw) = u^2w^2 &= e \\
u^{-1} &= u \\
w^{-1} &= w \\
(uw)^{-1} = w^{-1}u^{-1} = wu &= uw
\end{aligned}
$$

By Lagrange theorem, 4 must divides $|G|$, but $|G| = 2n$ and n is odd, $2n$ is not divisible by 4, so it's impossible to have two or more elements of order 2. In conclusion, there is only one element of order 2 in G.