Abstract Algebra I

Homework 6

Due: 12th November 2025
B13902024 張沂魁

We begin this exercise sheet with a definition that really should have been introduced alongside the notion of a centralizer. Let G be a group, and X be the set containing all the subgroups of G. If G acts by conjugation on X, then the subgroup of G fixing $H \in X$ is called the *normalizer of* H, and it is denoted by

$$N_G(H) = \{g \in G : g^{-1}Hg = H\}.$$

Obviously H is normal in G if and only if $N_G(H) = G$.

Exercise 1 Let G be a finite group and H a p-subgroup of G, i.e., $|H| = p^m$ for some $m \geq 1$.

(a) Let H act on a finite set S and let S_0 denote the subset of S consisting of elements fixed by all $h \in H$, i.e., $h \cdot x = x$. Show that $|S| \equiv |S_0| \pmod{p}$.

(b) Prove that $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

(c) If $p \mid [G : H]$, prove that $N_G(H) \neq H$.

Solution:

(a) Since we have

$$S_0 = \{x \in S \mid h \cdot x = x \quad \forall h \in H\},$$

so we have $x \in S_0$ iff $O(x) = \{x\}$. Hence, we can partition S into distinct orbits, i.e.

$$S = S_0 \cup \bigcup_{i=1}^{n} O_i,$$

where $|O_i| \geq 2$ for all $1 \leq i \leq n$, and by orbit-stabilizer theorem we know

$$2 \leq |O_i| \mid |H| = p^m \quad \forall 1 \leq i \leq n,$$

so $p \mid |O_i|$ for all $1 \leq i \leq n$, and since

$$|S| = |S_0| + \sum_{i=1}^{n} |O_i|,$$

so we know $|S| \equiv |S_0| \mod p$.

(b) If we let $S = \{gH : g \in G\}$, then $|S| = |G/H|$. Now we can define a group action of H on S by

$$h \cdot (gH) = (hg)H,$$

then we can similarly define

$$S_0 = \{x \in S : h \cdot x = x \quad \forall h \in H\} = \{gH \in S : (hg)H = gH \quad \forall h \in H\}.$$

Hence,

$$\begin{aligned} gH \in S_0 &\iff hgH = gH \quad \forall h \in H \iff g^{-1}hgH = H \quad \forall h \in H \\ &\iff g^{-1}hg \in H \quad \forall h \in H \iff g^{-1}Hg \subseteq H \iff g^{-1}Hg = H. \end{aligned}$$

Note that the last step holds since H is finite and thus $|g^{-1}Hg| = |H|$. Now since $g^{-1}Hg = H$ iff $g \in N_G(H)$, so $gH \in S_0$ iff $g \in N_G(H)$. Hence,

$$S_0 = \{gH \in S \mid g \in N_G(H)\} = N_G(H)/H.$$

Now by (a) we know $|S| \equiv |S_0| \mod p$, so we know

$$|G/H| \equiv |N_G(H)/H| \mod p \iff [G : H] \equiv [N_G(H) : H] \mod p.$$

(c) If $p \mid [G : H]$, then $[G : H] \equiv 0 \mod p$, which means $[N_G(H) : H] \equiv 0 \mod p$ by (b). This means

$$p \mid \frac{|N_G(H)|}{|H|},$$

and since $e \in N_G(H)$, so $|N_G(H)| > 0$, and thus

$$|H| < |N_G(H)|,$$

which means $N_G(H) \neq H$.

Exercise 2 If P is a Sylow p-subgroup of a finite group G, then

$$N_G(N_G(P)) = N_G(P).$$

Solution: Note that

$$N_G(P) = \left\{g \in G : g^{-1}Pg = P\right\}, \quad N_G(N_G(P)) = \left\{g \in G \mid g^{-1}N_G(P)g = N_G(P)\right\}.$$

We can notice that $P < N_G(P)$ and similarly $N_G(P) < N_G(N_G(P))$. Hence, $N_G(P) \subseteq N_G(N_G(P))$. Now we show that $N_G(N_G(P)) \subseteq N_G(P)$, and then we can conclude that $N_G(N_G(P)) = N_G(P)$. Suppose $|P| = p^e$, and if $g \in N_G(N_G(P))$, then $g^{-1}N_G(P)g = N_G(P)$, so we know $g^{-1}Pg \subseteq N_G(P)$ since $P < N_G(P)$. Now since $|g^{-1}Pg| = |P| = p^e$, so $P, g^{-1}Pg$ are both Sylow p-subgroups of $N_G(P)$. By Sylow's theorem, we know P and $g^{-1}Pg$ are conjugating in $N_G(P)$, i.e. $\exists h \in N_G(P)$ s.t.

$$g^{-1}Pg = h^{-1}Ph.$$

Hence, we have $(hg^{-1})\,P\,(gh^{-1}) = P$, so $gh^{-1} \in N_G(P)$ by definition, and thus $g \in N_G(P)$ since $h \in N_G(P)$ and $N_G(P)$ is a group. Hence, we showed that $N_G(N_G(P)) \subseteq N_G(P)$, and we're done.

Exercise 3 Let $p > q$ be distinct primes, and G a group of order $p^n q$ for $n \geq 1$. Prove that G contains a unique normal subgroup of index q.

Solution: If $Q \lhd G$ and $[G : Q] = q$, then we know

$$p^n q = |G| = q|Q|,$$

which gives $|Q| = p^n$, so Q is a Sylow p-subgroup fo G. Also, since $Q \lhd G$, so

$$g^{-1}Qg = Q \quad \forall g \in G.$$

Now if there is another $Q' \lhd G$ and $[G : Q'] = q$, then we know Q' is also a Sylow p-subgroup of G and thus by Sylow's theorem we have

$$Q' = g_1^{-1}Qg_1$$

for some $g_1 \in G$, and sicne $g_1^{-1}Qg_1 = Q$, so $Q^{-1} = Q$, so such Q is unique.

Now we show the existence. Since q is prime, so by Cauchy's theorem, we know there exists $g \in G$ s.t. $\mathrm{ord}(g) = q$, so $\langle g \rangle$ is a subgroup of G with order q.

Exercise 4 Prove that if every Sylow p-subgroup of a finite group G is normal for every prime p, then G is the direct product of its Sylow p-subgroups.

Solution: Now suppose $|G| = \prod_{i=1}^{k} p_i^{a_i}$ where p_i is a prime for all $1 \leq i \leq k$ and $p_i \neq p_j$ for all $i \neq j$. Now let P_i be a Sylow p_i-subgroup of G, then the problem conditions give $P_i \lhd G$ for all $1 \leq i \leq k$. Now we claim that for $i \neq j$, $P_i \cap P_j = \{e\}$. First note that $P_i \cap P_j < P_i$ and $P_i \cap P_j < P_j$, so by Lagrange's theorem, we know

$$|P_i \cap P_j| \mid p_i^{a_i}, \quad |P_i \cap P_j| \mid p_j^{a_j},$$

and since p_i and p_j are distinct prime, so we know $P_i \cap P_j = \{e\}$. Thus, the claim is true. Now note that we have

$$\begin{cases} P_i, P_j \lhd G \\ P_i \cap P_j = \{e\} \end{cases}, \quad \forall i \neq j,$$

so we know $P_iP_j \simeq P_i \times P_j$ and P_i and P_j commute, which has been proved during lecture. Now we claim that $S_v = P_1P_2 \dots P_v$ is a subgroup of G for all $1 \leq v \leq k$. Fix some v with $1 \leq v \leq k$. If $a, b \in S_v$, we suppose $a = c_1c_2 \dots c_v$ and $b = c_1'c_2' \dots c_v'$ where $c_i, c_i' \in P_i$ for all $1 \leq i \leq v$. Thus we know

$$ab = c_1c_1'c_2c_2' \dots c_vc_v' \in S_v$$

since P_i and P_j commute for distinct i, j. Besides, if $a = c_1c_2 \dots c_v \in S_v$ with $c_i \in P_i$ for all $1 \leq i \leq v$, then

$$a^{-1} = c_v^{-1}c_{v-1}^{-1} \dots c_1^{-1} = c_1^{-1}c_2^{-1} \dots c_v^{-1} \in S_v,$$

so we're done. Since this proof is true for all $1 \leq v \leq k$, so we're done. Now since for $H, K < G$, we have

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

so it sufficies to show that $|S_v| = |P_1||P_2| \dots |P_v|$ for all $1 \leq v \leq k$. We prove it by induction.

- Base case: $|S_1| = |P_1|$ is trivial.
- Now suppose $|S_{v-1}| = |P_1| \dots |P_{v-1}|$ for some $v > 1$, then we know

  $$|S_v| = |S_{v-1}P_v| = \frac{|S_{v-1}||P_v|}{|S_{v-1} \cap P_v|} = \frac{|P_1| \dots |P_v|}{|S_{v-1} \cap P_v|}.$$

  Now we show that $|S_{v-1} \cap P_v| = 1$. Since $S_{v-1} \cap P_v < S_{v-1}$ and $S_{v-1} \cap P_v < P_v$, so

  $$|S_{v-1} \cap P_v| \mid \gcd(|S_{v-1}|, |P_v|) = 1,$$

  which means $|S_{v-1} \cap P_v| = 1$. Hence, we know

  $$|S_v| = |P_1||P_2| \dots |P_v|,$$

  and we're done.

Hence, pick $v = k$, we have

$$|S_k| = |P_1| \dots |P_k| = |G|,$$

and since $S_k \subseteq G$, so we know $S_k = G$, which means $G = P_1P_2 \dots P_k$. Now we define a map

$$\varphi : G \to P_1 \times P_2 \times \cdots \times P_k, \quad \varphi(g) = (c_1, c_2, \dots, c_k), \text{ where } g = c_1c_2 \dots c_k \text{ with } c_i \in P_i.$$

We first show that this map is well-defined. Since $|G| = |P_1 \dots P_k|$, so we know if $g \in G$ has

$$g = c_1c_2 \dots c_k = c_1'c_2' \dots c_k'$$

with $c_i, c_i' \in P_i$ for all $1 \leq i \leq k$, then $c_i = c_i'$ for all $1 \leq i \leq k$. Hence, φ is well-defined. Now we show φ is an isomorphism. Since

$$|G| = |P_1 \times P_2 \times \cdots \times P_k|,$$

and φ is surjective (for $d = (c_1, \dots, c_k) \in P_1 \times P_2 \times \cdots \times P_k$, so $\varphi(c_1c_2 \dots c_k) = d$). Hence, φ is injective. Now we show that it is an homomorphism: If $g = c_1 \dots c_k$ anbd $h = c_1' \dots c_k'$ with $c_i, c_i' \in P_i$ for all $1 \leq i \leq k$. Then,

$$\begin{aligned}\varphi(gh) &= \varphi(c_1 \dots c_kc_1' \dots c_k') = \varphi(c_1c_1'c_2c_2' \dots c_kc_k') = (c_1c_1', c_2c_2', \dots, c_kc_k') \\ &= (c_1, c_2, \dots, c_k) \cdot (c_1', c_2', \dots, c_k') = \varphi(g)\varphi(h),\end{aligned}$$

so we're done. Hence, we know

$$G \simeq P_1 \times P_2 \times \cdots \times P_k.$$

Exercise 5 Prove that groups of order 30 and 105 are not simple.

Solution:

- Suppose G is a group of size 30, then since $30 = 2 \times 3 \times 5$, so if n_2, n_3, n_5 are the number of Sylow $2, 3, 5$-subgroups, respectively, we have

$$\begin{aligned} n_2 &\equiv 1 \mod 2 \\ n_3 &\equiv 1 \mod 3 \\ n_5 &\equiv 1 \mod 5, \end{aligned}$$

  and since if we define a group action by conjugacy, then by orbit-stabilizer theorem we know

$$n_2 \mid 30, \quad n_3 \mid 30, \quad n_5 \mid 30,$$

  and thus $n_2 = 1, 3, 5, 15$ and $n_3 = 1, 10$ and $n_5 = 1, 6$. If either $n_2, n_3, n_5 = 1$, then the Sylow $2, 3, 5$-subgroup is unique and by Sylow's theorem we know this group is normal in G, and thus G is not simple. Now suppose $n_2, n_3, n_5 > 1$. Note that for distinct Sylow 3-subgroup of G, say P_1, P_2, we claim that $P_1 \cap P_2 = \{1\}$. If $x \neq e$ and $x \in P_1 \cap P_2$, then since $\text{ord}(x) > 1$ and $\langle x \rangle$ is a subgroup of P_1 and P_2, so $\text{ord}(x) = 3$, and since $\langle x \rangle \subseteq P_1 \cap P_2$, so $P_1 \cap P_2 = P_1$ and $P_1 \cap P_2 = P_2$ ($|P_1| = |P_2| = 3 = |\langle x \rangle| = |P_1 \cap P_2|$). This means $P_1 = P_2$, which is a contradiction. Hence, $P_1 \cap P_2 = \{1\}$. Similar argument can be used on Sylow 5-subgroup. Hence, G has $10(3-1)$ elements of order 3 and $6(5-1)$ elements of order 5, which means G has at least

$$10(3-1) + 6(5-1) = 20 + 24 = 44 > 30$$

  elements, which is impossible, so G is not simple.

- Since $105 = 3 \times 5 \times 7$, so identical arguments of the case of group of size 30 can be stated here, which shows groups of size 105 is not simple.