# Abstract Algebra I

## Homework 7

B13902024 張沂魁

**Due: 19th November 2025**

For a finite group $G$ and a prime $p$ dividing $|G|$, let $n_p(G)$ denote the number of Sylow $p$-subgroups of $G$.

**Exercise 1** Let $G$ be a group of order 24, and suppose $n_2(G) > 1$.

(i) Prove that $G$ has a normal subgroup of order 4.

(ii) Is it possible that $n_3(G) > 1$?

**Solution:**

(i) Note that $24 = 2^3 \cdot 3$, and we know $n_2(G) \equiv 1 \mod 2$, so there are at least 3 Sylow 2-subgroup of $G$. Suppose they are $P_1, P_2, P_3$, and let $P = \{P_1, P_2, P_3\}$, then consider

$$\varphi : G \to S_3, \quad g \mapsto \varphi_g, \quad \text{where } \varphi_g(P_i) = gP_ig^{-1} \quad \forall i = 1, 2, 3.$$

Note that $\varphi$ is a homomorphism, and

$$\ker \varphi = \{g \in G : \varphi_g = 1\} = \left\{g \in G : gP_ig^{-1} = P_i \quad \forall i = 1, 2, 3\right\} = \bigcap_{i=1}^{3} N_G(P_i).$$

Now if we define a group action of $G$ on $P$ by $g \cdot P_i = gP_ig^{-1}$, then

$$\begin{aligned} \text{Stab}(P_i) &= \{g \in G : g \cdot P_i = P_i\} = \left\{g \in G : gP_ig^{-1} = P_i\right\} = N_G(P_i) \\ \text{Orb}(P_i) &= \{g \cdot P_i : g \in G\} = \left\{gP_ig^{-1} : g \in G\right\} = P. \end{aligned}$$

Hence, by orbit-stabilizer theorem, we know

$$|N_G(P_i)| = |\text{Stab}(P_i)| = \frac{|G|}{|P|} = 8,$$

and note that

$$P_i \subseteq N_G(P_i), \quad \text{and } |P_i| = |N_G(P_i)|,$$

so we know $P_i = N_G(P_i)$. Hence, $\ker \varphi = \bigcap_{i=1}^{3} N_G(P_i) = \bigcap_{i=1}^{3} P_i$. Note that $\text{Im}\varphi < S_3$, so by Lagrange's theorem:

– Case 1: $|\mathrm{Im}\varphi| = 1, 2, 3$, then by first isomorphism theorem,

$$|\ker\varphi| = \frac{|G|}{|\mathrm{Im}\varphi|} \geq 8,$$

but $\ker\varphi = \bigcap_{i=1}^{3} P_i$, and $|P_i| = 8$ for all $i = 1, 2, 3$. Hence, $P_1 = P_2 = P_3$, otherwise $|\ker\varphi| < 8$. However, $P_1, P_2, P_3$ are pairwise distinct, so this case is impossible.

– Case 2: $|\mathrm{Im}\varphi| = 6$, then $|\ker\varphi| = \frac{24}{6} = 4$, and thus $\ker\varphi$ is a normal subgroup of $G$ of order 4, and this is the only possible case, so we're done.

(ii) Consider $S_4$, then we know $|S_4| = 24$, and note that

| cycle types | $S_4$ |
|---|---|
| $(1)^4$ | 1 |
| $(2)(1)^2$ | 6 |
| $(3)(1)$ | 8 |
| $(4)$ | 6 |
| $(2)(2)$ | 3 |

Table 1: The number of permutations of [4] of different cycle types

If $n_2(S_4) = 1$, then there exists a normal subgroup of $S_4$ of order 8, but we can see from the above table that it is impossible such normal subgroup of $S_4$ exists since normal subgroups of $S_4$ are union of permutations of same cycle types. Hence, $n_2(S_4) > 1$. However, we know

$$\{(1)(2)(3)(4), (123), (132)\} \text{ and } \{(1)(2)(3)(4), (124), (142)\}$$

are both Sylow 3-subgroups of $S_4$, so it is possible that $n_3(G) > 1$.

**Exercise 2** Let $m$ be an odd integer and $G$ be a group of order $2m$. Consider the action of $G$ on itself via left multiplication; this induces a group homomorphism

$$\pi : G \to \mathrm{Perm}(G).$$

Recall that we have a group homomorphism

$$\mathrm{sgn} : \mathrm{Perm}(G) \to \{\pm 1\}$$

that sends each permutation to its sign.

(i) Show that the composition $\mathrm{sgn}\circ\pi : G \to \{\pm 1\}$ is surjective. *(Hint: Let $h$ be a generator of a Sylow 2-subgroup of $G$, and decompose $G$ into right cosets $\{e, h\}g_1, \ldots, \{e, h\}g_m$. Now consider $\pi(h)$.)*

(ii) Deduce that $G$ has a normal subgroup of order $m$.

**Solution:**

(i) Let $P \in \mathrm{Syl}_2(G)$, and suppose $P = \{e, h\}$, then since we know $\mathrm{sgn} \circ \pi(e) = +1$, so we just need to show that there exists some $x \in G$ s.t. $\mathrm{sgn} \circ \pi(e) = -1$. Now we claim that $\mathrm{sgn} \circ \pi(h) = -1$, and we're done. Note that

$$G = Pg_0 \cup Pg_1 \cup \cdots \cup Pg_{m-1},$$

where $g_0, g_1, \ldots, g_{m-1} \in G$ and we let $g_0 = e$. This is because $[G : P] = \frac{|G|}{|P|} = \frac{2m}{2} = m$, so we can write $G$ into union of $m$ right cosets of $P$. Hence, we know

$$G = \bigcup_{i=0}^{m-1} \{eg_i, hg_i\},$$

and if we define $\pi(h) = \pi_h$, then

$$\pi_h(g_i) = hg_i, \quad \text{and } \pi_h(hg_i) = h^2 g_i = g_i.$$

Thus, $\pi_h$ swaps $g_i$ and $hg_i$ for all $i$, i.e.

$$\pi(h) = (g_0 \quad hg_0)(g_1 \quad hg_1) \ldots (g_{m-1} \quad hg_{m-1}).$$

Note that $m$ is odd, so we know $\mathrm{sgn} \circ \pi(h) = -1$, and we're done.

(ii) Let $\varphi = \mathrm{sgn} \circ \pi$, then $\varphi$ is a homomorphism and $|\mathrm{Im}\varphi| = 2$ since $\varphi$ is surjective, and by first isomorphism theorem we know

$$|\ker \phi| = \frac{|G|}{|\mathrm{Im}\varphi|} = \frac{2m}{2} = m,$$

and $\ker \varphi \trianglelefteq G$, so we're done.

For the next two questions, the following fact will be helpful (try to prove it on your own): If $N$ is a normal subgroup of a group $G$ and a Sylow $p$-subgroup $P$ of $N$ is normal in $N$, then $P$ is normal in $G$.

**Proof of this fact:** For all $g \in G$, we have $|gPg^{-1}| = |G|$, and $gPg^{-1} \subseteq gNg^{-1} = N$ since $N \trianglelefteq G$, so $gPg^{-1} \in \mathrm{Syl}_p(N)$. Now since $P \trianglelefteq N$, so we know the Sylow $p$-subgroup of $N$ is unique, and thus

$$gPg^{-1} = P \quad \forall g \in G \implies P \trianglelefteq G.$$

**Exercise 3** et $G$ be a group of order 105.

(i) Show that $G$ has a normal subgroup $H$ of order 35.

(ii) Show that $H$ is cyclic.

(iii) Prove that $n_5(G) = n_7(G) = 1$.

**Solution:**

(i) Consider $n_5(G), n_7(G)$, then since $n_5(G) \equiv 1 \mod 5$ and thus $n_5(G) \mid \frac{|G|}{5}$, so we know $n_5(G) \in \{1, 21\}$, and similarly we can derive $n_7(G) \in \{1, 15\}$. Note that for distinct Sylow 5-subgroup of $G$, say $P, Q$, then $P \cap Q = \{1\}$ since $|P \cap Q| \mid 5$, and this statement holds also for Sylow 7-subgroups. Now if $n_7(G) = 15$ and $n_5(G) = 21$, then there are at least $(6-1)15+(5-1)21 > 105$ elements are in $G$, so either $n_5(G)$ or $n_7(G)$ is equal to 1. WLOG, suppose $n_5(G) = 1$ (if $n_7(G) = 1$, then it can be proved similarly.), and suppose $P \in \mathrm{Syl}_5(G)$ and $Q \in \mathrm{Syl}_7(G)$. Then, $P \trianglelefteq G$ and $Q < G$ and $P \cap Q = \{e\}$. Note that $PQ < G$ and

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = 5 \cdot 7 = 35.$$

Consider $G/P$, then $|G/P| = \frac{105}{5} = 21$. Note that $n_7(G/P) \equiv 1 \mod 7$ and this gives $n_7(G/P) \mid \frac{21}{7} = 3$, so we know $n_7(G) = 1$. Say $S \in \mathrm{Syl}_7(G/P)$, then $S \trianglelefteq G/P$. Suppose $\pi : G \to G/P$ is the map that $\pi(g) = gP$, then suppose $P' = \pi^{-1}(S)$ is the preimage of $S$ under $\pi$. Then, we have

$$|P'| = |S||P| = 7 \cdot 5 = 35$$

since $g_1 P = gP$ if and only if $g_1 = gp$ for some $p \in P$, and thus we have $|P|$ choices for $g_1$. Now we show that $P' \trianglelefteq G$ and then since $|P'| = 35$, so we're done. We first show that $P' < G$: If $x, y \in P'$, then $\pi(xy) = (xy)P = (xP)(yP) = \pi(x)\pi(y) \in S$ since $P \trianglelefteq G$. Also, if $x \in P'$, then $\pi\left(x^{-1}\right) = x^{-1}P = (xP)^{-1} \in S$. Thus, $P' < G$. Now we show that $P' \trianglelefteq G$: Suppose $g \in G$ and $p' \in P'$, then

$$\pi\left(gp'g^{-1}\right) = \pi(g)\pi\left(p'\right)\pi\left(g^{-1}\right) \in S$$

since $\pi\left(p'\right) \in S$ and $S \trianglelefteq G/P$. Hence, $gp'g^{-1} \in P'$, and thus $gP'g^{-1} = P'$ for all $g \in G$, and we're done.

(ii) Suppose $H \trianglelefteq G$ and $|H| = 35$. By (i), we know such $H$ exists. Thus, we know $n_5(H) = n_7(H) = 1$ by Sylow's theorem. Hence, suppose $P_5 \in \mathrm{Syl}_5(H)$ and $P_7 \in \mathrm{Syl}_7(H)$, then $P_5 \trianglelefteq H$ and $P_7 \trianglelefteq H$. Also, $P_5 \cap P_7 = \{e\}$. Hence,

$$|P_5 P_7| = \frac{|P_5| \cdot |P_7|}{|P_5 \cap P_7|} = 5 \cdot 7 = 35.$$

However, $P_5 P_7 \subseteq H$ and $|H| = 35$. Hence,

$$H = P_5 P_7 \simeq P_5 \times P_7 \simeq C_5 \times C_7 \simeq C_{35}$$

since $P_5, P_7 \trianglelefteq H$ and $5, 7$ are prime (so $P_5, P_7$ are cyclic) and $\gcd(5, 7) = 1$ (so $C_5 \times C_7 \simeq C_{35}$). Hence, $H$ is cyclic.

(iii) Continuing (ii). Since $P_5 \trianglelefteq H$ and $P_7 \trianglelefteq H$, and $H \trianglelefteq G$, so by the fact mentioned before this problem, we know $P_5 \trianglelefteq G$ and $P_7 \trianglelefteq G$. Also, $P_5, P_7$ are the Sylow 5-subgroup and the Sylow 7-subgroup of $G$, respectively. Hence, $n_5(G) = n_7(G) = 1$ since $P_5, P_7 \trianglelefteq G$.

**Exercise 4** More generally, let $G$ be a group of order $pqr$, where $p, q, r$ are distinct primes and $p < q < r$. We want to show that $n_r(G) = 1$.

(i) Suppose $n_r(G) > 1$. Show that $n_q(G) = 1$. Thus we deduce already that $G$ is not simple.

(ii) We now suppose $n_q(G) = 1$, and let $Q$ be the unique Sylow $q$-subgroup of $G$. Show that $G/Q$ has a normal subgroup of order $r$.

(iii) Deduce that $G$ has a normal subgroup of order $qr$ and conclude that $n_r(G) = 1$.

**Solution:**

(i) Since $n_r(G) \equiv 1 \mod r$ and $n_r(G) \mid \frac{pqr}{r} = pq$, so $n_r(G) \in \{1, p, q, pq\}$. Since $n_r(G) > 1$, and $n_r(G) \equiv 1 \mod r$, and $p, q < r$, so the only possibility is $n_r(G) = pq$. Hence, $\mathrm{Syl}_r(G)$ contributes $pq(r-1)$ elements of order $> 1$. Now if $n_q(G) > 1$, then since $n_q(G) \equiv 1 \mod q$ and $n_q(G) \mid \frac{pqr}{q} = pr$, so $n_q(G) \in \{p, r, pr\}$. Since $q > p$, so $p \not\equiv 1 \mod q$, so $n_q(G) \geq r$. Hence, $\mathrm{Syl}_q(G)$ contributes at least $r(q-1) = rq - r$ elements of order $> 1$. Also, $n_p(G) \geq 1$, so $\mathrm{Syl}_p(G)$ contributes at least $p - 1$ elements of order $> 1$. Hence, $G$ has at least

$$pq(r-1) + r(q-1) + p - 1 + 1 = pqr - pq + rq - r + p = pqr + (q-1)(r-p) > pqr$$

elements, which is impossible. Hence, $n_q(G) = 1$.

(ii) Note that $|G/Q| = pr$, then consider $n_r(G/Q)$, we know $n_r(G/Q) \equiv 1 \mod r$ and $n_r(G/Q) \mid \frac{pr}{r} = p$, so $n_r(G/Q) = 1$ since $p \not\equiv 1 \mod r$. Hence, suppose $R \in \mathrm{Syl}_r(G/Q)$, then $R \trianglelefteq G/Q$ since it is the unique Sylow $r$-subgroup of $G/Q$, and note that $|R| = r$, so we're done.

(iii) Consider the preimage of $R$ under the map $\pi : G \to G/Q$ where $\pi(g) = gQ$. Hence,

$$\left|\pi^{-1}(R)\right| = |R| \cdot |Q| = r \cdot q = qr$$

since $g_1 Q = gQ$ iff $g_1 = gq$ for some $q \in Q$. Now we show that $\pi^{-1}(R) \trianglelefteq G$, and thus $\pi^{-1}(R)$ is a subgroup of $G$ of order $qr$. We first show that $\pi^{-1}(R) < G$: If $x, y \in \pi^{-1}(R)$, then $\pi(xy) = xyQ = (xQ)(yQ) = \pi(x)\pi(y) \in R$ since $Q \trianglelefteq G$. Also, if $x \in \pi^{-1}(R)$, then $\pi\left(x^{-1}\right) = x^{-1}Q = (xQ)^{-1} \in R$, so we can conclude that $\pi^{-1}(R) < G$. Now we show that $\pi^{-1}(R) \trianglelefteq G$: If $x \in \pi^{-1}(R)$, then for all $g \in G$, $\pi\left(g^{-1}xg\right) = \left(g^{-1}xg\right)Q = \pi\left(g^{-1}\right)\pi(x)\pi(g) \in R$ since $\pi(x) \in R$ and $R \trianglelefteq G/Q$. Hence, $g^{-1}\pi^{-1}(R)g \subseteq \pi^{-1}(R)$ for all $g \in G$, and thus $\pi^{-1}(R) \trianglelefteq G$. Now we conclude that $n_r(G) = 1$. Since $n_r\left(\pi^{-1}(R)\right) \equiv 1 \mod r$ and $n_r\left(\pi^{-1}(R)\right) \mid \frac{qr}{r} = q$, and $q \not\equiv 1 \mod r$, so $n_r\left(\pi^{-1}(R)\right) = 1$. Now suppose $P_r$ is the unique Sylow $r$-subgroup of $\pi^{-1}(R)$, then since $\pi^{-1}(R) \trianglelefteq G$, so $P_r \trianglelefteq G$ by the fact before Exercise 3. Note that $P_r$ is also a Sylow $r$-subgroup of $G$, so $n_r(G) = 1$. Hence, if $n_r(G) > 1$, then by (i) (ii) (iii), we will show $n_r(G) = 1$, which is a contradiction, so we must have $n_r(G) = 1$.

**Exercise 5** Let $R$ be a commutative ring. We say an element $x \in R$ is a *zero divisor* if there is some nonzero element $y \in R$ such that $xy = 0$. If a ring has no nonzero zero divisors, we say the ring is an *integral domain*, or sometimes just *domain* for short.

(i) Classify all zero divisors of the following rings:

$$\mathbb{Z},\ \mathbb{Z}/6\mathbb{Z},\ \mathbb{Q},\ \mathbb{C}[x].$$

Which of them are integral domains? (You don't need to check they are commutative rings; addition and multiplication are carried out as usual.)

(ii) Show that any element in $R$ cannot be both invertible *and* a zero divisor at the same time.

(iii) However, an element may be neither invertible nor a zero divisor. Find an example.

(iv) Show that the invertible elements of the polynomial ring $R[x]$ coincide with the invertible elements of $R$.

**Solution:**

(i)
- $\mathbb{Z}$: If $xy = 0$ for $x, y \in \mathbb{Z}$ and $y \neq 0$, then $x = 0$, so the only zero divisor is 0, which means $\mathbb{Z}$ is an integral domain.
- $\mathbb{Z}/6\mathbb{Z}$: Note that the zero divisors are $[2], [3], [4], [0]$ since

$$[0] = [2] \cdot [3] = [3] \cdot [2] = [4] \cdot [3] = [0] \cdot [1].$$

Hence, $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

(ii) If $x \in R$ is invertible, then there exists $x^{-1}$ s.t. $xx^{-1} = 1$. Now if $x$ is a zero divisor, then $xy = 0$ for some $y \neq 0$, and thus

$$0 = x^{-1}(xy) = \left(x^{-1}x\right) y = y,$$

which is a contradiction. Hence, $x$ can not be a zero divisor if $x$ is invertible.

(iii) In $\mathbb{Z}$, 48763 is neither invertible nor a zero divisor.

(iv) If $f(x)$ is invertible in $R[x]$, then $\exists g(x) \in R[x]$ s.t. $f(x)g(x) = 1$. This implies $f, g$ must be constant polynomials. Hence, $f \in R$ and $f$ is invertible in $R$. Now if $p$ is invertible in $R$, then there exists $q \in R$ s.t. $pq = 1$. Then, since $f, g \in R[x]$, so $f$ is invertible in $R[x]$. Hence, we can conclude that invertible elements of $R[x]$ concide with those of $R$.