MA2202S Algebra I (S) Suggested Solutions

AY20/21 Semester 1

Author: Chong Jing Quan Reviewer: Pan Jing Bin

Question 1

(a) (i) Let $u \in \mathrm{Stab}(x)$. Then, $x = u \cdot x \in u \cdot A_0 \in \Omega$ so that $u \cdot A_0 \cap A_0 \neq \emptyset$. Thus, $u \cdot A_0 = A_0$, i.e. $u \in \mathrm{Stab}(A_0)$.

(ii) To prove $A_0 = X \implies \mathrm{Stab}(A_0) = G$:

For all $g \in G$, one has $g \cdot X = X$ by definition. Thus, $\mathrm{Stab}(A_0) = \mathrm{Stab}(X) = G$.

To prove $\mathrm{Stab}(A_0) = G \implies A_0 = X$:

Suppose $A_0 \subsetneq X$ but $\mathrm{Stab}(A_0) = G$. Pick $y \in X \setminus A_0$. By transitivity, there exists $g \in G$ such that $g \cdot x = y$. Thus $g \notin \mathrm{Stab}(A_0)$, which is a contradiction. Hence, $A_0 = X$.

To prove $A_0 = \{x\} \implies \mathrm{Stab}(A_0) = \mathrm{Stab}(x)$:

Let $u \in \mathrm{Stab}(A_0) = \mathrm{Stab}(\{x\})$. Then $u \cdot x = x$ so $u \in \mathrm{Stab}(x) \implies \mathrm{Stab}(A_0) \subseteq \mathrm{Stab}(x)$. By (a)(i), we already have $\mathrm{Stab}(x) \subseteq \mathrm{Stab}(A_0)$ so $\mathrm{Stab}(x) = \mathrm{Stab}(A_0)$.

To prove $\mathrm{Stab}(A_0) = \mathrm{Stab}(x) \implies A_0 = \{x\}$:

Assume for the sake of contradiction that there exists $y \neq x$ such that $y \in A_0$. By transitivity, there exists $g \in G$ such that $g \cdot x = y$. But $g \cdot A_0 \in \Omega$ and $g \cdot A_0 \cap A_0 \neq \emptyset$, so $g \cdot A_0 = A_0$, i.e. g stabilizes A_0 but not x. We have a contradiction. Hence, $A_0 = \{x\}$.

(iii) From part (a)(ii), it is easy to see that if $\{x\} \subsetneq A_0 \subsetneq X$ then $\mathrm{Stab}(x) \subsetneq \mathrm{Stab}(A_0) \subsetneq G$.

(b) (i) Since $1 \in H$, one has $\{x\} \subseteq A$. If $\{x\} = A$, then $H \subseteq \mathrm{Stab}(x)$, a contradiction. Thus, $\{x\} \subsetneq A$.

On the other hand, it is clear that $A \subseteq X$. I claim that there exists $g \in G \setminus H$ so that $g \cdot x \notin A$. Suppose otherwise, i.e. for each $g \in G \setminus H$, there exists $h \in H$ so that $g \cdot x = h \cdot x$. This means that $h^{-1}g \cdot x = x$, and so $h^{-1}g \in \mathrm{Stab}(x) \subsetneq H$. But $h(h^{-1}g) = g \in H$, a contradiction. This claim shows that $A \subsetneq X$.

(ii) Firstly, none of the sets in Ω is empty. Next, we show that $\bigcup_{g \in G} g \cdot A = X$. This is easy, because for each $y \in X$, there exists a $g \in G$ such that $y = g \cdot x \in g \cdot A$.

Then, we show that whenever $g_1 \neq g_2$, we either have $g_1 \cdot A \cap g_2 \cdot A = \emptyset$ or $g_1 \cdot A = g_2 \cdot A$.

Suppose $g_1 \cdot A \cap g_2 \cdot A \neq \emptyset$. We show that $g_2^{-1} g_1 \in H$. Pick $h_1, h_2 \in H$ such that $(g_1 h_1) \cdot x = (g_2 h_2) \cdot x$. Then,

$$(h_2^{-1} g_2^{-1} g_1 h_1) \cdot x = x \implies h_2^{-1} g_2^{-1} g_1 h_1 \in \mathrm{Stab}(x) \subsetneq H.$$

Thus, $g_2^{-1} g_1 = h_2 (h_2^{-1} g_2^{-1} g_1 h_1) h_1^{-1} \in H$. Now, for any $h \in H$, we see that

$$(g_1 h) \cdot x = (g_2 (g_2^{-1} g_1 h)) \cdot x \in g_2 \cdot A$$

and similarly

$$(g_2 h) \cdot x = (g_1 (g_1^{-1} g_2 h)) \cdot x \in g_1 \cdot A.$$

Hence, $g_1 \cdot A \subseteq g_2 \cdot A$ and $g_2 \cdot A \subseteq g_1 \cdot A$, which gives the desired equality.

Question 2

(a) Let $Q \in \mathrm{Syl}_p(H)$. I claim that $\exists R \in \mathrm{Syl}_p(G)$ such that $Q \leq R$.

By Sylow's first theorem, $\exists R' \in \mathrm{Syl}_p(G)$. By Sylow's second theorem, $\exists g \in G$ such that $gQg^{-1} \leq R' \implies Q \leq g^{-1}R'g$. But $g^{-1}R'g$ is also a Sylow-p subgroup of G and we are done.

Now suppose that $n_p(H) > n_p(G)$. Then $\exists Q_1, Q_2 \in \mathrm{Syl}_p(H)$ with $Q_1 \neq Q_2$, such that $\exists P \in \mathrm{Syl}_p(G)$ with $Q_1, Q_2 \leq P$. In particular, $Q_1, Q_2 \leq P \cap H \leq H$. Hence $P \cap H$ is a larger p-subgroup of H, which is a contradiction. The result follows.

(b) Consider the map $f : G \to G/N;\ g \mapsto gN$. Then f is a surjective homomorphism and has kernel N. Let $P \in \mathrm{Syl}_p(G)$. We will first prove that $f(P)$ is a Sylow p-subgroup of G/N. Firstly, note that $f(P) = \{pN \mid p \in P\} = PN/N$. But $|PN/N| = \frac{|P|}{|P \cap N|}$ is a power of p. Thus PN/N is a p-subgroup of G/N. Now observe that $[G : P]$ is relatively prime to p, so as $[G : PN]$. Hence, $[G/N : PN/N]$ is also relatively prime to p, implying that $f(P) = PN/N$ is a Sylow p-subgroup of G/N.

Now let Q be a Sylow p-subgroup of G/N. We will prove that $\exists P \in \mathrm{Syl}_p(G)$ such that $f(P) = Q$. By the Fourth Isomorphism Theorem, one can put $Q = \overline{Q}/N$ for some subgroup $\overline{Q}$ of G containing N. As such, $[G : \overline{Q}] = [G/N : Q]$ is relatively prime to p and so $\overline{Q}$ contains a Sylow p-subgroup P of G. By the Fourth Isomorphism Theorem again, $f(P) \leq f(\overline{Q}) = Q$. From above, we know that $f(P)$ is also a Sylow p-subgroup of G/N, which forces $f(P) = Q$.

This proves that $n_p(G/N) \leq n_p(G)$.

Remark. *One can generalize the problem statement by showing that $n_p(G/N) | n_p(G)$. A further strengthening of this result yields Hall's Theorem, i.e. $n_p(G) = n_p(N)n_p(G/N)n_p(T)$, where $T = N_{PN}(P \cap N)/P \cap N$.*

One can also generalize what is presented here by showing that if $f : G \to H$ is a surjective homomorphism, then $n_p(H) \leq n_p(G)$.

Question 3

(a) Without loss of generality, assume $o(g_i) = \infty$. Then, pick a non-identity element $g_j \in G_j$ so that the map $\psi : \langle g_i \rangle \to G_j$ defined by

$$\psi(g_i^a) \mapsto g_j^a$$

is a non-trivial homomorphism, a contradiction. Hence, the orders of $g_i \in G_i$ and $g_j \in G_j$ are finite.

Now, assume that the orders of g_i and g_j are not coprime to each other. Define$\psi : \langle g_i \rangle \to G_j$ by

$$\psi : g_i \to g_i^{o(g_i)/\gcd(o(g_i), o(g_j))},$$

which is a non-trivial homomorphism as $\gcd(o(g_i), o(g_j)) > 1$. We are done.

(b) Write $d_i := o(h_i)$ for each i. By part (a), $\gcd(d_i, d_j) = 1$ for $i \neq j$. By Chinese Remainder Theorem, the following system

$$\begin{aligned} x &\equiv 0 \pmod{d_1} \\ x &\equiv 0 \pmod{d_2} \\ &\vdots \\ x &\equiv 0 \pmod{d_{k-1}} \\ x &\equiv 1 \pmod{d_k} \end{aligned}$$

has a solution. Call the solution x_0. Then, $(h_1, h_2, \cdots, h_k)^{x_0} = (1, 1, 1, \cdots, h_k) \in H$.

(c) To prove $H \subseteq H_1 \times \cdots \times H_k$:

Let $(h_1, h_2, \cdots, h_k) \in H$. Using a similar argument in part (b), we see that for each i, we have $(1, 1, 1, \cdots, h_i, \cdots, 1) \in H$. This means that $h_i \in H_i$ and thus

$$(h_1, h_2, \cdots, h_k) \in H_1 \times H_2 \times \cdots H_k$$

The conclusion then follows.

To prove $H_1 \times \cdots \times H_k \subseteq H$:

Let $(h_1, h_2, \cdots h_k) \in H_1 \times \cdots \times H_k$. Then we have

$$\begin{gathered}(h_1, 1, \cdots, 1) \in H \\ (1, h_2, \cdots, 1) \in H \\ \vdots \\ (1, 1, \cdots, h_k) \in H\end{gathered}$$

and since H is a group,

$$(h_1, h_2, \cdots h_k) = (h_1, 1, \cdots, 1) * (1, h_2, \cdots, 1) * \cdots * (1, 1, \cdots, h_k) \in H.$$

(d) Suppose $H \trianglelefteq G$. Then,

$$(g_1, g_2, \cdots, g_k)(h_1, h_2, \cdots, h_k)(g_1, g_2, \cdots, g_k)^{-1} = (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}, \cdots, g_k h_k g_k^{-1})$$

so that $H_i \trianglelefteq G_i$ for each i. The argument for converse is similar.

(e) The subgroup to consider is

$$M := \{(1, 1, \cdots, \underbrace{h}_{i\text{-th position}}, \cdots, \underbrace{\phi(h)}_{j\text{-th position}}, 1, \cdots, 1) \mid h \in H_i\}.$$

It is easy to verify that M is a subgroup of G. It is also easy to see that this is one such counterexample as there exists $h_i \in H_i$ so that $\phi(h_i) \neq 1$. Thus $(1, 1, \cdots, h_i, \cdots, 1) \notin M$.

If we define each M_i in a similar way as in (c), then $h_i \notin M_i \implies M \not\subseteq M_1 \times \cdots \times M_k$.

Question 4

(a) Let $g \in G$. Then $gPg^{-1} \leq H$ and thus $gPg^{-1} \in \mathrm{Syl}_p(H)$. Then there exists $h \in H$ so that $gPg^{-1} = hPh^{-1} \implies h^{-1}gPg^{-1}h = P \implies h^{-1}g \in N_G(P)$. Thus $G = HN_G(P)$.

(b) By the Second Isomorphism Theorem, one has

$$G/H \cong HN_G(P)/H \cong N_G(P)/(H \cap N_G(P)) = N_G(P)/N_H(P).$$

(c) We induct on $|G|$. If G is nilpotent, then take $K = G$ and we are done. Henceforth, we may assume that G is not nilpotent.

Since G is not nilpotent, there is a Sylow p-subgroup P that is not normal in G, i.e. $N_G(P) \subsetneq G$. From part 2(b), the group PH/H is a Sylow p-subgroup of G/H. As G/H is nilpotent, by the Fourth Isomorphism Theorem, we get $PH \trianglelefteq G$. Since $P \in \mathrm{Syl}_p(G)$, certainly $P \in \mathrm{Syl}_p(PH)$.

Replacing H with PH in part (a) yields $G = PHN_G(P) = HN_G(P)$ and so by the Second Isomorphism Theorem, we get $G/H \cong N_G(P)/N_H(P)$. Since G/H is nilpotent, it follows that $N_G(P)/N_H(P)$ is nilpotent too.

By inductive hypothesis, there exists a nilpotent subgroup K of $N_G(P)$ such that $N_G(P) = N_H(P)K = KN_H(P)$. But from the modular law, we have

$$N_G(P) = KN_H(P) = K(H \cap N_G(P)) = KH \cap N_G(P),$$

i.e. $N_G(P) \subseteq KH = HK$. As $HN_G(P) = G$, we must have $G = HK$.

(d) We shall prove that if N is a non-trivial normal subgroup of nilpotent G, then $N \cap Z(G) \neq \{1\}$, so that the required statement follows by putting $N = H \cap K$ and $G = K$.

There are two methods of proving this statement, one uses upper central series, the other uses the properties of nilpotent groups.

Method 1. Since G is nilpotent, the upper central series terminates. For some positive integer n, one has $\zeta_n(G) = G$. In particular, there is $1 \le i \le n$ so that $N \cap \zeta_i(G) = \{1\}$ and $N \cap \zeta_{i+1}(G) \neq \{1\}$.

By the definition of upper central series, we have $\zeta_{i+1}(G)/\zeta_i(G) = Z(G/\zeta_i(G))$. Hence, for any $z \in \zeta_{i+1}(G)$ and $g \in G$, we have $zg\zeta_i(G) = gz\zeta_i(G)$, i.e. $[g, z] \in \zeta_i(G)$. This implies that $[G, \zeta_{i+1}(G)] \subseteq \zeta_i(G)$.

Before we proceed, we need the following lemma.

Lemma. If N_1 and N_2 are normal subgroups of a group G, then we have

$$[G, N_1 \cap N_2] \subseteq [G, N_1] \cap [G, N_2].$$

Proof. Let $g \in G$ and $n \in N_1 \cap N_2$ so that $gng^{-1}n^{-1} \in [G, N_1 \cap N_2]$. For $i = 1, 2$, we see that $n \in N_i$, thus $gng^{-1}n^{-1} \in [G, N_i]$. The result follows. □

As $[G, N] \le N$ by normality of N in G, from the lemma above, we obtain

$$[G, N \cap \zeta_{i+1}(G)] \subseteq [G, N] \cap [G, \zeta_{i+1}(G)] \subseteq N \cap \zeta_i(G) = \{1\}.$$

This implies that $N \cap \zeta_{i+1}(G) \subseteq Z(G) \implies N \cap \zeta_{i+1}(G) \subseteq N \cap Z(G)$ and since $N \cap \zeta_{i+1}(G) \neq \{1\}$, $N \cap Z(G) \neq \{1\}$.

Method 2. Define the sequence $N_0(G) = N, N_{i+1}(G) = [N_i(G), G]$ for integers $i \ge 1$. It is easy to see that $N_i(G) \le N$ for each positive integer i.

It is also clear that $N_0(G) = N \subseteq G = \gamma_0(G)$. I claim that $N_k(G) \subseteq \gamma_k(G)$. The case for $k = 0$ has been established. Assume that $N_n(G) \subseteq \gamma_n(G)$. Then one has

$$N_{n+1}(G) = [N_n(G), G] \subseteq [\gamma_n(G), G] = \gamma_{n+1}(G),$$

completing the inductive step.

But G is nilpotent, so there is a positive integer m such that $\gamma_m(G) = \{1\}$. Thus,

$$[N_{m-1}(G), G] = N_m(G) \subseteq \gamma_m(G) = \{1\}.$$

As such, one can find a positive integer k such that k is the smallest positive integer satisfying $N_k(G) = \{1\}$ and $N_{k-1}(G) \neq \{1\}$. This yields $N_{k-1} \subseteq Z(G)$ and so $N \cap Z(G) \neq \{1\}$.

(e) Assume $H \cap K \neq \{1\}$. By (d), we have

$$\{1\} \neq H \cap Z(K) \subseteq H \cap C_G(K) = \{1\},$$

a contradiction.

We now study the group $N_G(K)$. By definition, one has $K \trianglelefteq N_G(K)$. As $H \trianglelefteq G$, we use modular law and part (c) to get

$$N_G(K) = N_G(K) \cap G = N_G(K) \cap HK = K(N_G(K) \cap H) = (N_G(K) \cap H)K.$$

Since $H \cap K = \{1\}$, we have $(N_G(K) \cap H) \cap K = \{1\}$. Let $h \in N_G(K) \cap H$ and $k \in K$ and consider $hkh^{-1}k^{-1}$. Since $h \in N_G(K)$, $(hkh^{-1})k^{-1} \in K \subseteq N_G(K)$. On the other hand, H is normal so $h(kh^{-1}k^{-1}) \in H$. Thus we have $hkh^{-1}k^{-1} \in (N_G(K) \cap H) \cap K) = \{1\} \implies hk = kh$. Thus $N_G(K) \cap H \subseteq C_G(K)$. But $H \cap C_G(K) = \{1\}$, which implies $N_G(K) \cap H = \{1\}$ and so $N_G(K) = K$.