MA2202S - Algebra I (S) Suggested Solutions

(Semester 2, AY2023/2024)

Written by: Sarji Bona
Audited by: Thang Pang Ern

Question 1

Let G be a group. Assume G has a unique subgroup of order n, for some positive integer n. Denote this subgroup by H. Prove that H is a normal subgroup of G.

Solution: Let $g \in G$. Note that

$$\phi : G \to gHg^{-1} \quad \text{where} \quad h \mapsto ghg^{-1} \quad \text{is bijective,}$$

so $|gHg^{-1}| = |H| = n$. But $|H|$ is the unique subgroup of order n, so $gHg^{-1} = H$, which implies H is a normal subgroup of G. $\square$

Question 2

Let p be a prime. Prove that $a^p \equiv a \pmod p$ for any $a \in \mathbb{Z}$[1].

Solution: Consider the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}$. For each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, there exists a positive integer k such that $a^k = 1$. By Lagrange's theorem, $k \mid (p-1)$, so $p - 1 = km$ for some integer m. So $a^{p-1} = a^{km} = 1 \Rightarrow a^p = a$. Hence, $a^p \equiv a \pmod p$ for any $a \in \mathbb{Z}$. $\square$

Question 3

Let G be a p-group for some prime p with a normal subgroup H. Assume H is of order p. Prove that H is contained in the center of G.

Solution: Let the order of G be p^n for $n \in \mathbb{N}$. Note that $N_G(H)/C_G(H) = G/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$ which has order $p-1$. Since $p^n/|C_G(H)|$ divides $p-1$, $p^n/|C_G(H)|$ must be a power of p less than or equal to $p-1$, implying

$$p^n/|C_G(H)| = 1 \quad \text{so} \quad |C_G(H)| = p^n = |G| \quad \text{so} \quad C_G(H) = G.$$

Hence, all elements of H commute with all elements of G, thus, $H \subseteq Z(G)$. $\square$

[1] This is known as Fermat's little theorem

Question 4

Let G be a finite group. Let H and K be two subgroups of G such that $|H|$ and $|K|$ are coprime. We consider the natural (left) action of H on G/K. Prove that all the orbits have the cardinality $|H|$.

Solution: If $|H| = 1$, all orbit sizes must divide $|H|$ by the orbit-stabilizer theorem, so they must be all 1. If $|H| > 1$, let $|K| = n$, and h_1, h_2 be any two distinct elements of H, and $g \in G$. Then,

$$h_1 gK = h_2 gK \quad \text{so} \quad g^{-1}h_2^{-1}h_1 g \in K \quad \text{so} \quad (g^{-1}h_2^{-1}h_1 g)^n = e \quad \text{so} \quad g^{-n}h_2^{-n}h_1^n g^n = e.$$

Hence, $(h_2^{-1}h_1)^n = e$. So, the order of $h_2^{-1}h_1$ divides both $|K|$ and $|H|$, which can only be 1, implying $h_1 = h_2$, a contradiction. Thus, for any $g \in G$, all $h_i gK$ are pairwise distinct for all $h_i \in H$. Therefore, all orbits have cardinality $|H|$. $\square$

Question 5

Let G be a group. Prove that if $|G| = 56$ then G is not simple.

Solution: For a prime p, let n_p be the number of distinct p-Sylow subgroups of G. By Sylow's third theorem,

$$n_7 \equiv 1 \pmod 7 \text{ and } n_7 \mid 56 \quad \text{so} \quad n_7 = 1 \text{ or } 8.$$

If $n_7 = 1$, then it has a normal 7-Sylow subgroup, implying G is not simple by Sylow's second theorem. Next, assume $n_7 = 8$, then there is 1 element of order 1 and $8 \cdot (7-1) = 48$ elements of order 7.

By Sylow's second theorem,

$$n_2 \equiv 1 \pmod 2 \text{ and } n_2 \mid 56 \quad \text{so} \quad n_2 = 1 \text{ or } 7.$$

If $n_2 = 1$, again G is not simple by Sylow's second theorem. If $n_2 = 7$, then there are 7 subgroups of order 8. Let H_1 and H_2 be two distinct 2-Sylow subgroups. Then 7 out of the 8 elements in H_1 have order $2, 4$, or 8. There is also at least 1 element in H_2 that is not in H_1, which has order $2, 4$, or 8. In total, there are at least $1 + 48 + 7 + 1 = 57$ elements in G, a contradiction. Thus, if $|G| = 56$, then G is not simple. $\square$

Question 6

Let G be a group. Prove that the diagonal subgroup $\Delta(G) = \{(g, g) \in G \times G\} \subset G \times G$ is normal in $G \times G$ if and only if G is abelian.

Solution: If G is abelian, then for any $(g_1, g_2) \in G \times G$ and $(g, g) \in \Delta(G)$, we have

$$(g_1, g_2)(g, g)(g_1^{-1}, g_2^{-1}) = (g_1 g g_1^{-1}, g_2 g g_2^{-1}) = (g_1 g_1^{-1} g, g_2 g_2^{-1} g) = (g, g) \in \Delta(G),$$

so $(g_1, g_2)\Delta(G)(g_1^{-1}, g_2^{-1}) \subseteq \Delta(G)$, implying $\Delta(G) \trianglelefteq G \times G$.

We then prove the forward direction by contraposition. Suppose G is not abelian, then there exist $a, b \in G$ such that $ab \neq ba \Rightarrow a \neq bab^{-1}$. So $(a, b)(a, a)(a^{-1}, b^{-1}) = (a, bab^{-1}) \notin \Delta(G)$ since $bab^{-1} \neq a$, implying that $\Delta(G)$ is not normal.

Therefore, $\Delta(G)$ is normal in $G \times G$ if and only if G is abelian. $\square$

Question 7

Let G be a group with a subgroup H of finite index. Assume H is abelian and $[G : H] = n$. Let $S = \{t_1, \dots, t_n\} \subset G$ be a complete set of the representatives of the cosets G/H. The left action of G on G/H induces a permutation on S, such that $gt_iH = t_{g(i)}H$ for any $g \in G$. Here we abuse notations, and denote the induced permutation of g by g as well.

We define a transfer map $\tau : G \to H$ as follows. For any $g \in G$ and $t_i \in S$, we write $gt_i = t_{g(i)}h_{i,g}$ for some $h_{i,g} \in H$ and $t_{g(i)} \in S$. We define $\tau(g) = h_{1,g} \dots h_{n,g}$.

(a) Show that τ is a group homomorphism.

(b) Show that τ is independent of the choice S of representatives, as well as the ordering of elements in S.

Solution:

(a) Note that for any $g \in G$ and $i \in \{1, 2, \dots, n\}$, $t_{g(i)}^{-1}gt_i \in H$. For any $g_1, g_2 \in G$, we have

$$\begin{aligned}
\tau(g_1)\tau(g_2) &= \prod_{i=1}^{n} t_{g_1(i)}^{-1} g_1 t_i \cdot \prod_{j=1}^{n} t_{g_2(j)}^{-1} g_2 t_j = \prod_{j=1}^{n} t_{g_1(g_2(j))}^{-1} g_1 t_{g_2(j)} \cdot \prod_{j=1}^{n} t_{g_2(j)}^{-1} g_2 t_j \\
&= \prod_{j=1}^{n} t_{g_1(g_2(j))}^{-1} g_1 t_{g_2(j)} t_{g_2(j)}^{-1} g_2 t_j = \prod_{j=1}^{n} t_{g_1(g_2(j))}^{-1} g_1 g_2 t_j \\
&= \tau(g_1 g_2).
\end{aligned}$$

Hence, τ is a group homomorphism. $\square$

(b) Let $S' = \{u_1, \dots, u_n\} \subset G$ be any complete set of the representatives of the cosets G/H. Define τ' similarly to τ but on S' instead. There exists a unique permutation $\sigma \in S_n$ such that $t_iH = u_{\sigma(i)}H$ for all $i \in \{1, 2, \dots, n\}$. Then for all $i \in \{1, 2, \dots, n\}$, there exists $h_i \in H$ such that $t_ih_i = u_{\sigma(i)}$.

Now let $g \in G$. Denote by g' the induced permutation of g on S' where $gu_iH = u_{g'(i)}H$ for all $i \in \{1, 2, \dots, n\}$. Then for all $i \in \{1, 2, \dots, n\}$, we have

$$u_{g'(\sigma(i))}H = gu_{\sigma(i)}H = gt_iH = t_{g(i)}H = t_{g(i)}h_{g(i)}H = u_{\sigma(g(i))}H,$$

so $g' \circ \sigma = \sigma \circ g$. Then

$$\begin{aligned}
\tau'(g) &= \prod_{i=1}^{n} u_{g'(i)}^{-1} g u_i = \prod_{i=1}^{n} u_{g'(\sigma(i))}^{-1} g u_{\sigma(i)} = \prod_{i=1}^{n} u_{\sigma(g(i))}^{-1} g t_i h_i = \prod_{i=1}^{n} (t_{g(i)} h_{g(i)})^{-1} g t_i h_i \\
&= \prod_{i=1}^{n} h_{g(i)}^{-1} t_{g(i)}^{-1} g t_i h_i = \left(\prod_{i=1}^{n} t_{g(i)}^{-1} g t_i \right) \left(\prod_{i=1}^{n} h_{g(i)}^{-1} \right) \left(\prod_{i=1}^{n} h_i \right) = \prod_{i=1}^{n} t_{g(i)}^{-1} g t_i \\
&= \tau(g).
\end{aligned}$$

Therefore, τ is independent of S. $\square$