Adv Abstract Algebra: AAA #Practice Midterm

Due on 2022 at 11:59PM

Prof. Peter Hermann Spr 2022

Xianzhi

2023

Practice Midterm

Problem 1

Let $H \leq G$ and $A \leq G$ such that $|G : H| = 3$ and $|A| = 85$. Prove that

1. $A \leq H$.
2. $\cap_{g\in G} g^{-1}Hg \neq 1$.

Solution:

Part A

Observe that the right cosets of H partitions G into equivalent classes, so $x \sim y \iff xy^{-1} \in H$.
(Why? say $x, y \in Hb$ for some $b \in G$, then $x = h_1 b$ and $y = h_2 b$ then

$$\begin{aligned} xy^{-1} &= h_1 b(h_2 b)^{-1} && (1)\\ &= h_1 bb^{-1}h_2^{-1} && (2)\\ &= h_1 h_2^{-1} \in H && (3) \end{aligned}$$

Thus, if we restrict this partition into equivalent class to A, it's still a partition. Let $u, v \in A$, since $A \cap H \leq A$, we have u, v in some coset w.r.t. $A \cap H \iff uv^{-1} \in A \cap H$ which means uv^{-1} in A and in H.
since uv^{-1} is automatically in A because A is a group,

$$\begin{aligned} uv^{-1} \in A \cap H &\iff uv^{-1} \in H && (4)\\ &\iff u, v \text{ in the same coset w.r.t. } H \text{ in } G && (5) \end{aligned}$$

This observation implies the number of $A \cap H$ cosets in A is at most the # of H cosets in G, which is 3, since $|G : H| = 3$.
Since # of $A \cap H$ cosets in A need to divide the order of $|A| = 85$, this number cannot be 3 or 2, so it must be 1. Thus, $|A : A \cap H| = 1$, and since $A \cap H \leq A$, we conclude $A \cap H = A \implies A \cap H \supseteq A$ which implies $A \leq H$.

Part B

We show $a \in \cap_{g\in G} g^{-1}Hg$. Take any $a \in A$. Observe that if we let $\mathcal{R}$ be the set of all right cosets of H, then for $g \in G$, we define $g^\rho \in Sym\mathcal{R} = S_3$ by $g^\rho : Hx \mapsto Hxg$ then $\rho : G \xrightarrow{\rho} Sym\mathcal{R} = S_3$ is a homomorphism because $g \to g^\rho$. and $g \in G$ is acting on the right cosets of H in G by right multiplication, and $ker\rho = \cap_{g\in G} g^{-1}Hg$.
If $x \in \cap_{g\in G} g^{-1}Hg$, then for all cosets of H, Hb, we can write $x = b^{-1}h_1 b$ for some $h_1 \in H$. So $Hb \to Hbx = Hbb^{-1}h_1 b = Hh_1 b = Hb$, which is the identity permutation, so $x \in ker\rho$ implies $ker\rho \supseteq \cap_{g\in G} g^{-1}Hg$. If $x \in ker\rho$, then for all Hb, we have $Hb = Hbx \implies H = Hbxb^{-1}$, thus, $bxb^{-1} \in H \implies bxb^{-1} = h_2$ for some $h_2 \in H$.
$\implies x = b^{-1}h_2 b \in \cap_{g\in G} g^{-1}Hg$
$\implies ker\rho \subseteq \cap_{g\in G} g^{-1}Hg$
Thus, $ker\rho = \cap_{g\in G} g^{-1}Hg$.
We show for any $a \in A, a \in ker\rho$. Let $a \in A \implies |a| \mid |A| = 85$, Also $|\rho(a)|$ divide $|S_3| = 3! = 6$.
Let $|a| = k$, so $a^k = 1$.
then $(\rho(a))^k = \rho(a^k) = \rho(1) = 1$, so $|\rho(a)|$ divide k.
Thus, $|\rho(a)|$ divide $gcd(85, 6) = 1$.
so $|\rho(a)| = 1 \implies \rho(a) = 1$
so a is in $ker\rho$.
Thus, $A \subseteq ker\rho$, so $ker\rho \neq 1 \implies \cap_{g\in G} g^{-1}Hg \neq 1$.

Problem 2

Assume that $\langle c\rangle \lhd G$, $|G : \langle c\rangle| = 3$, c has infinite order, and some $b \in G$ has order 3. Prove that $G = \langle c, b\rangle$ and $G \cong \mathbb{Z}^+ \times \mathbb{Z}_3^+$. (For any ring S, the additive group of S is denoted by S^+.

Solution:

$\langle c\rangle \lhd G$, $|G : \langle c\rangle| = 3$, since $\langle c\rangle$ is infinite cyclic group (c has infinite order), any element that is non identity has infinite order. Thus, $b \notin \langle c\rangle$, since $|b| = 3$.
Thus, we can form distinct cosets $\langle c\rangle$, $b\langle c\rangle$, $b^2\langle c\rangle$.
$b\langle c\rangle$ and $b^2\langle c\rangle$ are distinct, since if $b\langle c\rangle = b^2\langle c\rangle$, then $b^{-1}b^2 \in \langle c\rangle$,
$\implies b \in \langle c\rangle$. Contradiction.
Since $|G : \langle c\rangle| = 3$, we found all $\langle c\rangle$ cosets.
since G is partitioned into cosets, we have $G = \langle c\rangle \cup b\langle c\rangle \cup b^2\langle c\rangle$, and elements $g \in G$ is in one of the cosets, and can be written as $b^i c^j$, and since $\langle c\rangle \lhd G$, the left, right cosets of $\langle c\rangle$ in G are the same, so G is indeed generated by $\langle c, b\rangle$.
It's clear that $\langle c\rangle \lhd G, \langle b\rangle \cap \langle c\rangle = 1$, and since G is generated by $\langle c, b\rangle$, and $\langle c\rangle$ is normal, so $\langle b\rangle \cdot \langle c\rangle$ is a group, so $\langle b\rangle \cdot \langle c\rangle \leq G$. but any $g \in G$ can be written as $b^i c^j$, if it's $c^j b^i$, then use normality of $\langle c\rangle$ to get $b^{i'} c^{j'}$. Thus, we only need to show $\langle b\rangle \lhd G$, then G is the internal direct product of $\langle c\rangle$ and $\langle b\rangle$, so it's isomorphic to the external direct product $\langle c\rangle \times \langle b\rangle$, then since $\langle c\rangle \times \langle b\rangle \cong \mathbb{Z}^+ \times \mathbb{Z}_3^+$, by sending $c \mapsto 1$ in $\mathbb{Z}^+$, and $b \mapsto 1$ in $\mathbb{Z}_3^+$.
so $G \cong \langle c\rangle \times \langle b\rangle \cong \mathbb{Z}^+ \times \mathbb{Z}_3^+$.
Show $\langle b\rangle \lhd G$.

Problem 3

Prove that $\mathbb{Q}^+$ (the additive group of the rational numbers) is hopfian.
Hint. If $H \lneqq \mathbb{Q}^+$ and $|H| > 1 \implies \exists n \in H$ such that n is a positive integer and $\frac{1}{n} \notin H$. Then $\frac{1}{n} + H$ has finite order in $\mathbb{Q}^+/H$.

Solution:
We want to show take any subgroup that is not 1, and not $\mathbb{Q}^+, H \leq \mathbb{Q}^+$, then $\mathbb{Q}^+/H \ncong \mathbb{Q}^+$.
since $\mathbb{Q}^+$ is abelian, anysubgroup is normal.
Thus, we take a proper $H \leq \mathbb{Q}^+, H \neq \mathbb{Q}^+, |H| > 1$, observe that $|H| = \infty$, since if $h \neq e, h \in H$, then all $(h + h + h + \ldots)$ with $nh \in H$, so H has infinite many elements. Thus, for some sufficient large positive integer $m \in H$, we have $1/m \notin H$. This is possible since $H \neq \mathbb{Q}^T$. Thus, we could consider coset $1/m + H$. This coset has finite order in $\mathbb{Q}^+/H$, since $m^2(\frac{1}{m} + H) = m^2\frac{1}{m} + H = m + H = H$, so $|\frac{1}{m} + H|$ divides m^2, so $|\frac{1}{m} + H| < \infty$. However, every non identity element $q \in Q^{-1}$ has infinite order, since adding q to itself many times will never get to zero. Thus, there cannot be an isomorphism between $\frac{Q^+}{H}$ and $\mathbb{Q}^+$, since Isomorphism preserves order of the element. We can also obtain a direct contradiction. say $\exists \phi \frac{Q^+}{H} \mapsto Q^+$. such that $\phi(\frac{1}{m} + H) = q \in \mathbb{Q}$ and $q \neq 1$. Let $|\frac{1}{m} + H| = k < \infty$, then $1 = \phi(1) = \phi\left((\frac{1}{m} + H)^k\right) = \phi(\frac{1}{m} + H)^k = q^k$ thus q has finite order. Contradiction.

Problem 4

Let a group G have order $5^2 \cdot 7 \cdot 37$. Show that

1. G has a unique Sylow 37-subgroup $\mathbb{Q}$.
2. $Q \leq Z(G)$.
3. The mapping $f : G \to G,\ \forall g \in G,\ g \to g^{175}$ is a homomorphism. What is the image of f?

Solution:

G has order $5^2 \cdot 7 \cdot 37$, show G has unique Sylow 37-subgroup Q, let $n_{37} = \#$ of Sylow 37 subgroup in G, by Sylow theorem,

$$n_{37} \equiv 1 \mod 37 \text{ and} \tag{6}$$
$$n_{37} \text{ divide } 5^2 \cdot 7 = 175, \tag{7}$$

possible choices: $1, 5, 7, 25, 35, 175$, but among those, only 1 satisfy $1 \equiv 1 \mod 37$. so $n_{37} = 1$, so G has unique Sylow 37 subgroup, we call $\mathbb{Q}$.

Part A

G acts on $\mathbb{Q}$ by conjugation, and since unique Sylow-p subgroup is also normal, $\mathbb{Q} \triangleleft G$, thus, $\forall g \in G$, $g^{-1}Qg \subseteq Q$, and since $h^{-1}(g^{-1}Qg)h = (gh)^{-1}Qgh$, this conjugation action could be associated with automorphism on Q.

$$G \xrightarrow{\varphi} Aut(Q) \leq Sym(Q) \tag{8}$$
$$g \xrightarrow{\varphi} fg \text{ where } Q^{fg} = g^{-1}Qg \subset Q \tag{9}$$

similar to a proof in class, $Q \leq Z(G) \iff$ this action is trivial $\iff \varphi$ is trivial: φ maps G to the identity automorphism on Q.
$\iff Im\varphi = \{e\}$.
Thus, we show $Q \leq Z(G)$ by showing $Im\varphi = \{e\}$. By 1st Iso Thm

$$G/ker\varphi \cong Im\varphi \implies \frac{|G|}{|ker\varphi|} = |Im\varphi| \qquad \implies |Im\varphi| \text{ divide } |G| = 5^2 \cdot 7 \cdot 37 \tag{10}$$

On the other hand, $Im\varphi \leq Aut(Q)$.
Since $|Q| = 37$, which is prime $\implies Q$ is cyclic $\implies Q$ is abelian.
thus, except identity, all elements of Q has order 37, and there are 36 of such elements, so $|Aut(Q)| = 36$.
Let $Q = \langle a \rangle$.

$$37 = \text{order}(a^i) = \frac{\text{order}(a) = 37}{gcd(37, i)} \implies gcd(37, i) = 1 \tag{11}$$

implies there are 36 such i satisfy this.
Thus, $|Im\varphi|$ divide $|Aut(Q)| = 36$.
Thus, $|Im\varphi|$ divide both 36 and $5^2 \cdot 7 \cdot 37$
$\implies |Im\varphi|$ divide $gcd(36, 5^2 \cdot 7 \cdot 37) = 1 \implies |Im\varphi| = 1 \implies Im\varphi = \{e\}$.

Part B

Since Q is the unique Sylow 37 subgroup, Q is normal, so get factor group $|G/Q| = 175$, since $Imf = \{g^{175} \mid g \in G\}$. Let $g \in G$

$$Qg^{175} = (Qg)^{175} = e_{G/Q} = Q \tag{12}$$

which implies $g^{175} \in Q, \implies Imf \subset Q$. Since f is homomorphism, *why?* Imf is a subgroup of $G \implies Imf \leq Q$, thus, $|Imf|$ divide $|Q| = 37 \implies |Imf| = 1$ or 37.
Assume $|Imf| = 1 \implies Imf = \{e\} \implies \left\{g^{175} | g \in G\right\} = \{e\}$, so for all $g \in G, g^{175} = e \implies |g|$ divide 175, but we know $e \neq q \in Q$ has order 37 since Q is prime order cyclic group, and $37 \nmid 175$. Contradiction.
$\implies |Imf| = 37$. Combine with $Imf \leq Q \implies Imf = Q$.

Problem 5

Let G be a group (infinite or finite). Let $A \neq 1$ be an abelian subgroup of G such that $|G : A| = 5$.
Show that G has some nontrivial normal subgroup.

Solution:

Consider the action of G on the set of right cosets of $A : \mathcal{R}$

$$G \xrightarrow{\rho} Sym\mathcal{R} \tag{13}$$
$$g \to g^\rho \tag{14}$$
$$g^\rho : Ab \to Abg \tag{15}$$

By 1st iso thm:

$$G/ker\rho \cong Im\rho \leq S_5 \tag{16}$$
$$|G/ker\rho| = |Im\rho| \text{ divide } |S_5| = 5! = 120 \tag{17}$$

first, observe that $ker\rho$ cannot be the whole group G, because if $\rho(G) = 1$, then this contradicts ρ action transitively on the five cosets of A in G.
If $|G| > 5!$ then since $|G/ker\rho|$ divides $5!$, we conclude $ker\rho > 1$. So we are done in this case.

If $|G| \leq 5!$, then we observe if we let $|G| = k \leq 5!$, k must have a factor of 5, since $|G : A| = 5, \implies 5 \mid k$.
Thus, there exists a Sylow 5-group, we call S.
If # of S is 1, we are done, since unique S is normal.
If # of S is not 1, let's consider it's possibilities.

$$\# \text{ of } S \equiv 1 \mod 5 \tag{18}$$
$$\# \text{ of } S \mid \frac{k}{5}, \tag{19}$$
$$\frac{k}{5} \leq \frac{120}{5} = 24 \tag{20}$$

Since $\frac{k}{5}$ can be any number in $\{1, 2, \ldots, 24\}$,
of S could be $6, 11, 17, 22$.

If # of S is 6, then we consider Syl_3 subgroup in A, since $|A|$ has a factor of 3. (because $6 \mid \frac{k}{5}$). Then since Syl_3 subgroup are conjugates of each other, if $\exists!$ Syl_3 subgroup, we done, if not, there are 5 of them, because there are 5 cosets of A, but $5 \equiv 2 \mod 3$, which is a contradiction, so $\exists!$ Syl_3 subgroup which is normal. Other case can be done similarly.
for p instead of 3, provided $5 \not\equiv 1 \mod p$, *i.e.,* $p \neq 2$.