Algebraic Structures- Solutions of Homework 6

written by Motke Porat

December 2017

1 Question 1.

1.1 (e):

- Clearly if $k = 1$ then $X_1 = \{(1)\}$ is a subgroup of S_n.
- If $k > 1$, then $(1) \notin X_k$ and then X_k is not a subgroup of S_n.
- For every $\sigma \in S_n$ and a cycle $(a_1, ..., a_k) \in X_k$, we have

  $$\sigma^{-1}(a_1, ..., a_k)\sigma = (\sigma(a_1), ..., \sigma(a_k)) \in X_k,$$

  therefore

  $$\begin{aligned} \sigma^{-1}X_k\sigma &= \{\sigma^{-1}(a_1, ..., a_k)\sigma : a_1 \neq ... \neq a_k \in \{1, ..., n\}\} \\ &= \{(\sigma(a_1), ..., \sigma(a_k)) : a_1 \neq ... \neq a_k \in \{1, ..., n\}\} = X_k \end{aligned}$$

  and as a corollary it is easy to see that $\langle X_k \rangle \lhd S_n$, as

  $$\sigma^{-1}(g_1 \cdot ... \cdot g_m)\sigma = (\sigma^{-1}g_1\sigma) \cdot ... \cdot (\sigma^{-1}g_m\sigma) \in \langle X_k \rangle$$

  for every $\sigma \in S_n$ and $g_1, ..., g_m \in X_k$ (which imply that $\sigma^{-1}g_j\sigma \in X_k$ for all $j = 1, ..., m$).

1.2 (h):

Let $A \in GL_2(\mathbb{C})$, we know that A has two eigenvalues $\lambda_1, \lambda_2 \in \mathbb{C}$ (might be equal) and its Jordan form might be of the forms:

$$\begin{pmatrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{pmatrix}, \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{pmatrix}$$

if $\lambda_1 = \lambda_2$, and

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

if $\lambda_1 \neq \lambda_2$. In addition we know that for every $B \in GL_2(\mathbb{C})$, the Jordan form of $B^{-1}AB$ is equal to the Jordan form of A and therefore these are all the conjugacy classes.

1.3 (i):

For every $a \in G$, we have the following

$$\begin{aligned} x \in a^{-1}N_G(H)a &\iff axa^{-1} \in N_G(H) \iff (axa^{-1})^{-1}H(axa^{-1}) = H \\ &\iff x^{-1}(a^{-1}Ha)x = a^{-1}Ha \iff x \in N_G(a^{-1}Ha), \end{aligned}$$

so we proved that $a^{-1}N_G(H)a = N_G(a^{-1}Ha)$.

2 Question 2.

2.1 (d):

Let G be a finite group, $\phi : G \to G$ be an automorphism such that $\phi(x) = x$ if and only if $x = e$, and assume that $\phi \circ \phi = Id$. Define the mapping $\psi : G \to G$ by

$$\psi(x) = \phi(x)x^{-1}.$$

The mapping ψ is $1-1$: For every $x_1, x_2 \in G$,

$$\psi(x_1) = \psi(x_2) \Longrightarrow \phi(x_1)x_1^{-1} = \phi(x_2)x_2^{-1} \Longrightarrow \phi(x_2^{-1}x_1) = x_2^{-1}x_1$$

and the last part implies that $x_2^{-1}x_1 = e \Longrightarrow x_1 = x_2$. As G is finite and $\psi : G \to G$ is $1-1$, it follows that ψ is onto G, therefore for every $g \in G$, there exists $x \in G$ for which

$$g = \phi(x)x^{-1} \Longrightarrow \phi(g) = \phi(\phi(x)) \cdot \phi(x^{-1}) = x \cdot \phi(x^{-1}) = g^{-1}.$$

Then we got that $\phi(g) = g^{-1}$ is an automorphism of G, so for every $a, b \in G$:

$$\phi(ab) = \phi(a)\phi(b) \Longrightarrow (ab)^{-1} = a^{-1}b^{-1} = (ba)^{-1} \Longrightarrow ab = ba$$

which means that G is commutative (abelian).

2.2 (g):

- As $\mathbb{Z}$ is generated by either 1 or -1, if $\phi \in Aut(\mathbb{Z})$ then $\phi(1) = 1$ or $\phi(1) = -1$. and in any case $\phi(n) = \phi(1)n$; so-

$$Aut(\mathbb{Z}) = \{\phi_1, \phi_2\} \approx \mathbb{Z}_2, \quad \phi_1(n) = n, \phi_2(n) = -n, \quad n \in \mathbb{Z}.$$

- The group $\mathbb{Z}_n$ is generated by an element $a \in \mathbb{Z}_n$ if and only if $(a, n) = 1$, therefore ψ must map the generator 1 to one of the $\phi(n)$-many generators of $\mathbb{Z}_n$, so

$$Aut(\mathbb{Z}_n) = \{\psi_a : (a, n) = 1\}, \quad \psi_a(\overline{k}) = \overline{a} \cdot \overline{k}.$$

- As S_3 is generated by the 2 permutations (12) and (123), i.e., $S_3 = \langle (12), (123) \rangle$, then $\phi \in Aut(S_3)$ if and only if $\phi((12))$ is of order 2 in S_3 and $\phi((123))$ is of order 3 in S_3. Therefore, $\phi((12))$ can be equal to $(12), (13)$ or (23), while $\phi((123))$ can be equal to (123) or (132), and these are exactly all the possibilities for building ϕ, so we have 6 elements in

$Aut(S_3)$. To show that $Aut(S_3) \approx S_3$, it is enough to show that $Aut(S_3)$ is not commutative, since a not commutative group of order 6 must be isomorphic to S_3. Consider the following 2 elements in $Aut(S_3)$ defined by

$$\phi_1((12)) = (12), \phi((123)) = (132)$$

and

$$\phi_2((12)) = (13), \phi_2((123)) = (123),$$

so it is easily seen that $\phi_1((13)) = \phi_1((12)(123)) = (12)(132) = (23)$ and

$$\phi_2\phi_1((12)) = \phi_2((12)) = (13), \quad \phi_1\phi_2((12)) = \phi_1((13)) = (23),$$

which implies that $\phi_1\phi_2 \neq \phi_2\phi_1$ so $Aut(S_3)$ is not commutative.

3 Question 3.

3.1 (a):

As $|G| = 36 = 2^2 3^3$, we know from the Sylow's theorems that

$$n_2, n_3 \mid 36, n_2 = 1(mod\, 2) \text{ and } n_3 = 1(mod\, 3),$$

which imply that $n_3 = 1$ or $n_3 = 4$.

- If $n_3 = 1$, it means that there exists a unique subgroup of G of order 9, so this subgroup is a normal subgroup and we are done.
- If $n_3 = 4$, there are 4 subgroups of G of order 9, say

  $$Sylp_3(G) = \{P_1, P_2, P_3, P_4\}$$

  and set $N := P_1 \cap P_2 \cap P_3 \cap P_4$. For every $g \in G$ and $1 \leq i \leq 4$, $P_i^g := g^{-1} P_i g \in Sylp_3(G)$ and clearly $P_i^g \neq P_j^g$ for $i \neq j$, then we get that

  $$N^g = \bigcap_{i=1}^{4} P_i^g = \bigcap_{j=1}^{4} P_j = N,$$

  i.e., that $N \lhd G$. Moreover, we must have $|N| \mid 9$ and so $|N| = 1, 3$ or 9.
- If $|N| = 9$, it means that $N \subseteq P_i$ and $|N| = |P_i|$ so $N = P_i$ for every $1 \leq i \leq 4$ and then $P_1 = P_2 = P_3 = P_4$ and that is a contradiction.
- We will now show that $|N| > 1$: Define the mapping $\phi : G \to S_4$ by

  $$(\phi(g))(i) = j \text{ if and only if } P_i^g = P_j.$$

  so this ϕ is a group homomorphism as,

  $$(\phi(gh))(i) = j \iff P_i^{gh} = P_j \iff (P_i^g)^h = P_j \iff (\phi(g)\phi(h))(i) = j.$$

For every $1 \leq i \leq 4$, we know that $4 = n_3 = [G : N_G(P_i)]$ and hence $|N_G(P_i)| = 9 = |P_i|$, which implies that $N_G(P_i) = P_i$. Therefore,

$$\ker(\phi) = \{g \in G : P_i^g = P_i \, \forall 1 \leq i \leq 4\} = \bigcap_{i=1}^{4} N_G(P_i) = \bigcap_{i=1}^{4} P_i = N$$

and the first homomorphism theorem implies that

$$G/N = G/\ker(\phi) \approx Im(\phi) \leq S_4 \Longrightarrow \frac{36}{|N|} \mid 24 \Longrightarrow |N| > 1.$$

Therefore $|N| > 1 \Longrightarrow |N| = 3$ and we are done.

3.2 (f):

Define the following function $\phi : G \to Sym(G/H)$ by $\phi(g) := \phi_g$, where

$$\phi_g(aH) = (ga)H, \quad \forall a \in G.$$

This ϕ is a group homomorphism, as for every $g_1, g_2, a \in G$ we have

$$\phi_{g_1 g_2}(aH) = (g_1 g_2 a)H = \phi_{g_1}((g_2 a)H) = \phi_{g_1} \circ \phi_{g_2}(aH).$$

Moreover, if $g \in \ker(\phi)$ then $\phi_g = Id$ which means that $(ga)H = aH$ for every $a \in G$, in particular for $a = e$ we get that $gH = H$ and hence $g \in H$. Therefore,

$$N := \ker(\phi) \leq H$$

and clearly $N \lhd G$ as N is the kernel of a group homomorphism. It only remains to show that $N \neq \{e\}$: If $N = \{e\}$, then

$$G \approx \phi(G) \leq Sym(G/H) \Longrightarrow n = |G| \mid |Sym(G/H)| = k!$$

and this is a contradiction.

3.3 (g):

- Let us write $|G| = p^a k$ where $(p, k) = 1$, then we have $|P| = p^a$. As $P \leq H$, we know that $p^a \mid |H|$, so we can write $|H| = p^b m$ with $(p, m) = 1$ and $b \leq a$. On the other hand, $H \leq G$ so $p^b m \mid p^a k$ which implies that $a \geq b$. Finally, we got

$$|H| = p^a m, |P| = p^a \Longrightarrow P \in Syl_p(H).$$

- Take $G = S_4, H = A_4$, so $|G| = 24, |H| = 12$. If $P \in Syl_2(H)$ then $|P| = 2^2 = 4$ and such a subgroup can not be in $Syl_2(G)$, since then $|P| = 2^3 = 8$.