NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Teo Wei Hao

MA2202 Abstract Algebra I
AY 2005/2006 Sem 2

Question 1

(a) If $k \in \mathbb{Z}$ such that $m \mid k$ and $n \mid k$, then there exists $a, b \in \mathbb{Z}$ such that $am = bn = k$.
Also as $\gcd(m, n) = 1$, there exists $s, t \in \mathbb{Z}$ such that $sm + tn = 1$. This give us,

$$\begin{aligned} k &= k(sm + tn) \\ &= bn(sm) + am(tn) \\ &= mn(bs + at). \end{aligned}$$

Thus $mn \mid k$.

(b) Since $p \mid k^2$, by Euclid's Lemma, we have $p \mid k$. Similarly, $q \mid k$.
Together with the fact that p and q are distinct primes, we have $pq = \operatorname{lcm}(p, q) \mid k$.

Question 2

(a) We have $\alpha = \begin{pmatrix} 1 & 2 & 4 & 10 & 5 & 9 & 8 & 6 \end{pmatrix}\begin{pmatrix} 3 \end{pmatrix}\begin{pmatrix} 7 \end{pmatrix}$.
Thus $\operatorname{sgn}(\alpha) = (-1)^{10-3} = -1$ and $\alpha^{-1} = \begin{pmatrix} 1 & 6 & 8 & 9 & 5 & 10 & 4 & 2 \end{pmatrix}$.

(b) We have,

$$\begin{aligned} \alpha\beta\alpha^{-1} &= \begin{pmatrix} \alpha(2) & \alpha(6) & \alpha(1) & \alpha(3) \end{pmatrix} \\ &= \begin{pmatrix} 2 & 7 & 3 & 5 \end{pmatrix}. \end{aligned}$$

Question 3

(a) As $HK = KH$ is non-empty, we can let $a_1, a_2 \in HK$.
This implies that there exists $h_1, h_2 \in H$, $k_1, k_2 \in K$ such that $a_1 = h_1k_1$, $a_2 = h_2k_2$.
Since K is a group, there exists $k_3 \in K$ such that $k_3 = k_1k_2^{-1}$.
Since $HK = KH$, there exists $h_3 \in H$, $k_4 \in K$ such that $h_3k_4 = k_3h_2^{-1}$.
Lastly since H is a group, there exists $h_4 \in H$ such that $h_4 = h_1h_3$.
Thus we have $a_1a_2^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1k_3h_2^{-1} = h_1h_3k_4 = h_4k_4 \in HK$.
Therefore $HK \leq G$.

(b) For any $h \in H$, $k \in K$, we have $(kh)^{-1} = h^{-1}k^{-1} \in HK$. Since $HK \leq G$, we have $kh \in HK$.
Thus $KH \subseteq HK$.
We have $k^{-1}h^{-1} \in KH \subseteq HK$. Thus there exists $h' \in H$, $k' \in K$ such that $k^{-1}h^{-1} = h'k'$.
This give us $hk = \left(k^{-1}h^{-1}\right)^{-1} = (h'k')^{-1} = k'^{-1}h'^{-1} \in KH$, i.e. $HK \subseteq KH$.
Therefore $HK = KH$.

Question 4

(a) Let $G = A_4$, and $H = \langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rangle \leq G$.
We have $\begin{pmatrix} 1 & 4 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 \end{pmatrix} \notin H$.
Thus $\begin{pmatrix} 1 & 4 & 2 \end{pmatrix} H \neq \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} H$.
However, $\begin{pmatrix} 1 & 4 & 2 \end{pmatrix} \left(\begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \right)^{-1} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \in H$.
This give us $H \begin{pmatrix} 1 & 4 & 2 \end{pmatrix} = H \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix}$.

(b) Our given condition is equivalent to if $a, b \in G$ such that $aH = bH$, then $Ha = Hb$.
For all $g \in G$, $h \in H$, let $ghg^{-1} = k$, i.e. $gh = kg$. This give us $gH = ghH = kgH$.
Thus, we have $Hg = Hkg$, i.e. $k = (kg)\left(g^{-1}\right) \in H$. Therefore $H \lhd G$.

Question 5

(a) Let $f : G/(H \cap K) \to G/H \times G/K$ be such that $f(g(H \cap K)) = (gH, gK)$.
Now for $g_1, g_2 \in G$, we have

$$\begin{aligned} (g_1H, g_1K) = (g_2H, g_2K) &\Leftrightarrow g_1^{-1}g_2 \in H \text{ and } g_1^{-1}g_2 \in K \\ &\Leftrightarrow g_1^{-1}g_2 \in H \cap K \\ &\Leftrightarrow g_1(H \cap K) = g_2(H \cap K). \end{aligned}$$

Thus f is a well-defined injective function. Therefore,

$$\begin{aligned} |G/(H \cap K)| &\leq |G/H \times G/K| \\ [G : H \cap K] &\leq [G : H] \cdot [G : K]. \end{aligned}$$

Note: Here $G/H, G/K$ and $G/(H \cap K)$ are not quotient groups, but are just sets of left cosets.

(b) By Lagrange's Theorem, $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$, thus $|H \cap K| \mid \gcd(|H|, |K|)$.
In particular, $|H \cap K| \leq \gcd(|H|, |K|) \leq a|H| + b|K|$ for any $a, b \in \mathbb{Z}$.
Since $\gcd([G : H], [G : K]) = 1$, there exists $s, t \in \mathbb{Z}$ such that

$$\begin{aligned} s\left(\frac{|G|}{|H|}\right) + t\left(\frac{|G|}{|K|}\right) &= 1 \\ |G|\left(s|K| + t|H|\right) &= |H| \cdot |K|. \end{aligned}$$

Thus, we get $|G| \cdot |H \cap K| \leq |G| \cdot \gcd(|H|, |K|) \leq |G|\left(s|K| + t|H|\right) = |H| \cdot |K|$.
Rearranging, we get $[G : H] \cdot [G : K] = \dfrac{|G|^2}{|H| \cdot |K|} \leq \dfrac{|G|}{|H \cap K|} = [G : H \cap K]$.
Combining with (5a), we get $[G : H \cap K] = [G : H] \cdot [G : K]$.

Question 6

Let the 10 stripes be vertically orientated, and numbered 1 to 10 from left to right respectively.
Let $C = \{c_1, c_2, c_3, c_4\}$ be the set of 4 colours.
Let set $X = \{(a_1, a_2, \ldots, a_{10}) \mid a_i \in C, i = 1, 2, \ldots 10\}$ correspond to the colouring given to stripe 1 to 10 in that order. We notice that colouring $(a_1, a_2, \ldots, a_9, a_{10})$ is identical to $(a_{10}, a_9, \ldots, a_2, a_1)$.

Thus let group $G = \langle \begin{pmatrix} 1 & 10 \end{pmatrix} \begin{pmatrix} 2 & 9 \end{pmatrix} \begin{pmatrix} 3 & 8 \end{pmatrix} \begin{pmatrix} 4 & 7 \end{pmatrix} \begin{pmatrix} 5 & 6 \end{pmatrix} \rangle$.

We define an action $\alpha : G \times X \to X$ such that $\alpha_g(a_1, a_2, \ldots a_{10}) = (a_{g(1)}, a_{g(2)}, \ldots, a_{g(10)})$.
The number of orbits N correspond to the number of distinct flags. Now,

$$N = \frac{1}{2}\left[\text{Fix}\,(1_G) + \text{Fix}\,\left(\begin{pmatrix} 1 & 10 \end{pmatrix}\begin{pmatrix} 2 & 9 \end{pmatrix}\begin{pmatrix} 3 & 8 \end{pmatrix}\begin{pmatrix} 4 & 7 \end{pmatrix}\begin{pmatrix} 5 & 6 \end{pmatrix}\right)\right].$$

Every $x \in X$ is fixed by 1_G, and thus $\text{Fix}(1_G) = 4^{10}$.
For $\begin{pmatrix} 1 & 10 \end{pmatrix}\begin{pmatrix} 2 & 9 \end{pmatrix}\begin{pmatrix} 3 & 8 \end{pmatrix}\begin{pmatrix} 4 & 7 \end{pmatrix}\begin{pmatrix} 5 & 6 \end{pmatrix}$ to fix x, x must have the same colour for each cycle. Therefore, $\text{Fix}\left(\begin{pmatrix} 1 & 10 \end{pmatrix}\begin{pmatrix} 2 & 9 \end{pmatrix}\begin{pmatrix} 3 & 8 \end{pmatrix}\begin{pmatrix} 4 & 7 \end{pmatrix}\begin{pmatrix} 5 & 6 \end{pmatrix}\right) = 4^5$.
This give us $N = \frac{1}{2}(4^{10} + 4^5) = 524800$.

Therefore there are 524800 distinct flags in total.

Question 7

(a) Let $a \in G$ such that $G/Z(G) = \langle aZ(G)\rangle$. For any $g \in G$, there exists $k \in \mathbb{Z}$ such that $g \in a^k Z(G)$.
Thus there exists $z \in Z(G)$ such that $g = a^k z$.
This give us $ag = a\left(a^k z\right) = a^{k+1}z = a^k(az) = a^k(za) = \left(a^k z\right)a = ga$, i.e. $a \in Z(G)$.
Therefore we have $[G : Z(G)] = 1$, i.e. $G = Z(G)$.

(b) Let $f : G \to H$ be the surjective function $f(\sigma) = \tau_\sigma$.
For $g \in G$, we have $(\tau_{\sigma_1} \cdot \tau_{\sigma_2})(g) = \tau_{\sigma_1}\left(\sigma_2 g \sigma_2^{-1}\right) = \sigma_1\sigma_2 g \sigma_2^{-1}\sigma_1^{-1} = \tau_{\sigma_1\sigma_2}(g)$.
Thus $f(\sigma_1\sigma_2) = \tau_{\sigma_1\sigma_2} = \tau_{\sigma_1} \cdot \tau_{\sigma_2} = f(\sigma_1) \cdot f(\sigma_2)$. This give us f to be a homomorphism.

Now

$$\begin{aligned} \ker(f) &= \{\sigma \in G \mid \tau_\sigma = 1_H\} \\ &= \{\sigma \in G \mid \sigma g \sigma^{-1} = g, g \in G\} \\ &= \{\sigma \in G \mid \sigma g = g\sigma, g \in G\} \\ &= Z(G). \end{aligned}$$

Therefore by First Isomorphism Theorem, we have $G/Z(G) \simeq H$.

Question 8

(a) Let $S = \{g \in G, g^2 \neq 1_G\}$ and $T = \{g \in G, g^2 = 1_G\}$ and $|S| = 2r$. Thus we can rename the elements of G to be in $S = \left\{s_1, s_1^{-1}, s_2, s_2^{-1}, \ldots, s_r, s_r^{-1}\right\}$ and $T = \{t_1, t_2, \ldots, t_{n-2r}\}$.

Now since G is abelian, we have $x = s_1 s_1^{-1} s_2 s_2^{-1} \cdots s_r s_r^{-1} t_1 t_2 \cdots t_{n-2r} = t_1 t_2 \cdots t_{n-2r}$.
Thus again as G is abelian, we have $x^2 = t_1^2 t_2^2 \cdots t_{n-2r}^2 = 1_G$.

(b) We are given that $T = \{1_G, b\}$. Thus using result of (8a.), we get $x = 1_G b = b$.

(c) If $y^2 \equiv 1 \mod p$, then $p \mid \left(y^2 - 1\right) = (y-1)(y+1)$.
Since p is prime, by Euclid's Lemma, $p \mid y - 1$ or $p \mid y + 1$, i.e. $y \equiv 1 \mod p$ or $y \equiv -1 \mod p$.

Let us consider the group $(\mathbb{Z}/p\mathbb{Z})^*$. As established above, we have $x = [1]_p$ and $x = [-1]_p$ to be the only solutions to $x^2 = [1]_p$. Since $p \neq 2$, $[1]_p \neq [-1]_p$. Thus from (8b.), we get $[(p-1)!]_p = [1]_p[2]_p \cdots [p-1]_p = [-1]_p$, i.e. $(p-1)! \equiv -1 \mod p$.