NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Teo Wei Hao

MA2202 Algebra I
AY 2003/2004 Sem 2

Question 1

Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A$.
We have,

$$\begin{aligned}
[(a_1,b_1) * (a_2,b_2)] * (a_3,b_3) &= \left(a_1a_2, b_1a_2 + a_1^{-1}b_2\right) * (a_3,b_3) \\
&= \left(a_1a_2a_3, b_1a_2a_3 + a_1^{-1}b_2a_3 + a_1^{-1}a_2^{-1}b_3\right), \\
(a_1,b_1) * [(a_2,b_2) * (a_3,b_3)] &= (a_1,b_1) * \left(a_2a_3, b_2a_3 + a_2^{-1}b_3\right) \\
&= \left(a_1a_2a_3, b_1a_2a_3 + a_1^{-1}b_2a_3 + a_1^{-1}a_2^{-1}b_3\right).
\end{aligned}$$

Thus $[(a_1,b_1) * (a_2,b_2)] * (a_3,b_3) = (a_1,b_1) * [(a_2,b_2) * (a_3,b_3)]$, i.e. $(A,*)$ is associative.
$(1,0) * (a,b) = (a,b) * (1,0) = (a,b)$ for all $(a,b) \in A$, thus $(1,0) \in A$ is the identity in $(A,*)$.
For all $(a,b) \in A$, as $a \neq 0$, we have $\left(a^{-1}, -b\right) \in A$.
Since $(a,b) * \left(a^{-1}, -b\right) = \left(a^{-1}, -b\right) * (a,b) = (1,0)$, it is the inverse of (a,b) in $(A,*)$.

Therefore, $(A,*)$ is a group.

We have $(2,1), (2,0) \in A$. Now $(2,1) * (2,0) = (4,2)$ but $(2,0) * (2,1) = \left(4, \frac{1}{2}\right)$.
Thus $(A,*)$ is not abelian.

Question 2

H is non-empty since $1_{S_n} \in H$.
Let $\sigma_1, \sigma_2 \in H$, this give us $\sigma_2^{-1}(n) = n$. Thus we have $\sigma_1\sigma_2^{-1}(n) = \sigma_1(n) = n$, and thus $\sigma_1\sigma_2^{-1} \in H$.
Therefore $H \leq S_n$.

Question 3

Since G is non-cyclic, $G \neq 1_G$, and so there exists $a \in G - \{1_G\}$ with $\{1_G\} < \langle a \rangle < G$.
Thus there exists $b \in G - \langle a \rangle$.
This give us $\langle b \rangle \neq \langle a \rangle$, and since $b \neq 1_G$, we can get $\{1_G\} < \langle b \rangle < G$.
Now by Lagrange's Theorem, $|\langle a \rangle| \mid |G|$ and $|\langle b \rangle| \mid |G|$.
However $|\langle a \rangle|, |\langle b \rangle| \neq |G|$, and thus $|\langle a \rangle| \leq \frac{1}{2}|G|$ and $|\langle b \rangle| \leq \frac{1}{2}|G|$.
As $\langle a \rangle$ and $\langle b \rangle$ are subgroups of G, we get $\{1_G\} \leq \langle a \rangle \cap \langle b \rangle$.
Thus by Principle of Inclusion-Exclusion, we have

$$\begin{aligned}
|\langle a \rangle \cup \langle b \rangle| &= |\langle a \rangle| + |\langle b \rangle| - |\langle a \rangle \cap \langle b \rangle| \\
&\leq \frac{1}{2}|G| + \frac{1}{2}|G| - 1 \\
&< |G|.
\end{aligned}$$

Thus $G - (\langle a \rangle \cup \langle b \rangle)$ is non-empty, i.e. there exists $c \in G - (\langle a \rangle \cup \langle b \rangle)$.
We have $\langle c \rangle \neq \langle a \rangle$ and $\langle c \rangle \neq \langle b \rangle$ and $c \neq 1_G$, which lead us to conclude that $\{1_G\} < \langle c \rangle < G$.
Therefore for any group G, we can construct 3 non-trivial subgroups, namely $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$.

Question 4

Since G is cyclic, there is exactly one subgroup, say H, of G such that $|H| = m$. H is also cyclic. Thus for all $g \in G$ such that $\circ(g) = m$, we must have $\langle g \rangle = H$, i.e. $g \in H$.

Since H is cyclic, there exists $a \in H$ such that $\langle a \rangle = H$.
Let $k, d \in \mathbb{Z}^+$ be such that $\gcd(k, m) = d$. Thus $a^{\frac{k}{d}} \in H$ and $\left(a^k\right)^{\frac{m}{d}} = \left(a^{\frac{k}{d}}\right)^m = 1_H$.
This implies that if $d > 1$, then $\circ\left(a^k\right) \leq \frac{m}{d} < m$.
If $d = 1$, then we let $r \in \mathbb{Z}^+$ be such that $\left(a^k\right)^r = 1_H$. This implies that $m \mid kr$.
By consequence of Euclid's Lemma, $m \mid r$. Thus from what we have established, $\circ\left(a^k\right) = m$.

Therefore $\circ\left(a^k\right) = m$ iff $\gcd(k, m) = 1$, and thus there are $\varphi(m)$ such elements in G.

Question 5

Let $G_n = \langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 3 & 4 \end{pmatrix}, \ldots, \begin{pmatrix} n-2 & n-1 & n \end{pmatrix} \rangle$, $n \in \mathbb{Z}^+$.
It is direct that $G_n \subseteq A_n$.
Let P_n be the statement that $A_n \subseteq G_n$, $n \in \mathbb{Z}^+$.

$A_1 = A_2 = \{1_{S_n}\} = G_1 = G_2$. Thus P_1 and P_2 are trivially true.
Consider P_3. We have $A_3 = \{\begin{pmatrix} 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 & 1 \end{pmatrix}\} = G_3$. Thus P_3 is true.

Now assume that P_k is true for some $k \in \mathbb{Z}^+$, $k \geq 3$. Consider P_{k+1}.
Let $\alpha \in A_{k+1}$, and $\alpha(k+1) = i$.
If $i = k+1$, then we let $\beta = \alpha$, and so $\beta(k+1) = k+1$.
If $i = k$, then we let $\beta = \begin{pmatrix} k-1 & k & k+1 \end{pmatrix} \alpha$, which give us $\beta(k+1) = k+1$.
If $i < k$, then we let

$$\beta = \begin{pmatrix} k-1 & k & k+1 \end{pmatrix} \begin{pmatrix} k-1 & k & k+1 \end{pmatrix} \begin{pmatrix} k-2 & k-1 & k \end{pmatrix} \cdots \begin{pmatrix} i & i+1 & i+2 \end{pmatrix} \alpha,$$

which give us $\beta(k+1) = k+1$.

Notice that β is a product of elements in G_{k+1} and α, thus to get $\alpha \in G_{k+1}$, it suffice to show that $\beta \in G_{k+1}$. Now β does not move $k+1$, thus $\beta \in S_k$. Since α is an even permutation, β is a product of even permutations, and thus is also an even permutation. This give us $\beta \in A_k$.
Thus by induction hypothesis, $\beta \in G_k \subseteq G_{k+1}$. Hence $\alpha \in G_{k+1}$, i.e. $A_{k+1} \subseteq G_{k+1}$.

Therefore $A_n = G_n$ for all $n \in \mathbb{Z}^+$.

Question 6

Let $a \in G \backslash \{1_G\}$.
By Lagrange's Theorem, $\circ(a) \mid p^n$, and thus we can write $\circ(a) = p^k$ for some $k \in \mathbb{Z}^+$, $k \leq n$.
Now notice that $\left(a^{p^{k-1}}\right)^p = a^{p^k} = 1_G$, i.e. $\circ\left(a^{p^{k-1}}\right) \mid p$.
However $a^{p^{k-1}} \neq 1_G$ as $\circ(a) \nmid p^{k-1}$, and so $\circ\left(a^{p^{k-1}}\right) \neq 1$.
This give us $\circ\left(a^{p^{k-1}}\right) = p$, i.e. we can always constructed an element of order p from G.

Question 7

Let $\circ(g) = p$ be prime, and let there exists $a \in \langle g \rangle \cap H$ such that $a \neq 1_G$.
Then there exists $k \in \mathbb{Z}^+$ such that $a = g^k \in H$. Since $a \neq 1_G$, we have $p \nmid k$, and thus $\gcd(p, k) = 1$.

This give us $s, t \in \mathbb{Z}$ such that $sp + tk = 1$. Since H is a group, we have

$$\begin{aligned} g &= g^{sp+tk} \\ &= (g^p)^s \left(g^k\right)^t \\ &= \left(g^k\right)^t \in H. \end{aligned}$$

Question 8

Let $h \in H$ and $g \in G$. We denote $a = ghg^{-1}$.
By condition given, there exists $h_1, h_2 \in H$ such that $g^2 = h_1$ and $(gh)^2 = h_2$. Thus,

$$\begin{aligned} (gh)(gh) &= (ag)(gh) \\ h_2 &= ag^2h \\ &= ah_1h \\ a &= h_2h^{-1}h_1^{-1} \in H. \end{aligned}$$

Therefore $H \lhd G$.

Question 9

(a) Since $\left(a^{m-1}\right)(a) + (-1)(M) = a^m - M = 1$, we have $\gcd(a, M) = 1$. Thus $a \in \mathbb{Z}_M^*$.

For all $1 \leq i \leq m$, we have $\left(a^{m-i}\right)\left(a^i\right) + (-1)(M) = a^m - M = 1$, which give us $\gcd\left(a^i, M\right) = 1$. Thus $a^i \in \mathbb{Z}_M^*$. We notice that $a^m \equiv 1 \mod M$, thus $a^m = 1_{\mathbb{Z}_M^*}$.
Now since $a^m \geq 3$, we have $M \geq 2$ and $a \geq 2$. Hence for $1 \leq i < m$, $1 < a^i < M+1$, i.e. $a^i \neq 1_{\mathbb{Z}_M^*}$.
Thus $\circ(a) = m$ (as a by-product, we also can conclude that $\langle a \rangle \leq \mathbb{Z}_M^*$).

(b) From $M \mid a^n - 1$, we get $a^n \equiv 1 \mod M$, i.e. $a^n = 1_{\mathbb{Z}_M^*}$. Since $\circ(a) = m$, we have $m \mid n$.

Question 10

There are $\varphi(\varphi(19)) = \varphi(18) = 6$ primitive roots of 19.
Now, $18 = 2 \times 3^2$. Since,

$$\begin{aligned} 2^6 = 64 &\not\equiv 1 \mod 19; \\ 2^9 = 512 &\not\equiv 1 \mod 19, \end{aligned}$$

we conclude that 2 is a primitive root of unity modulo 19.

Now $(\mathbb{Z}/18\mathbb{Z})^* = \{[1]_{19}, [5]_{19}, [7]_{19}, [11]_{19}, [13]_{19}, [17]_{19}\}$. Since,

$$\begin{aligned} 2^5 &\equiv 13 \mod 19; \\ 2^7 &\equiv 14 \mod 19; \\ 2^{11} &\equiv 15 \mod 19; \\ 2^{13} &\equiv 3 \mod 19; \\ 2^{17} &\equiv 10 \mod 19, \end{aligned}$$

we have the primitive roots of unity modulo 19 to be $2, 3, 10, 13, 14, 15$.