NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Teo Wei Hao

MA2202 Algebra I
AY 2002/2003 Sem 2

Question 1

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

$$\begin{aligned}
[(a_1,b_1)*(a_2,b_2)]*(a_3,b_3) &= (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2)*(a_3,b_3) \\
&= (a_1a_2a_3 - b_1b_2a_3 - a_1b_2b_3 - b_1a_2b_3, a_1a_2b_3 - b_1b_2b_3 + a_1b_2a_3 + b_1a_2a_3), \\
(a_1,b_1)*[(a_2,b_2)*(a_3,b_3)] &= (a_1,b_1)*(a_2a_3 - b_2b_3, a_2b_3 + b_2a_3) \\
&= (a_1a_2a_3 - a_1b_2b_3 - b_1a_2b_3 - b_1b_2a_3, a_1a_2b_3 + a_1b_2a_3 + b_1a_2a_3 - b_1b_2b_3).
\end{aligned}$$

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.
Also $(a_1,b_1)*(a_2,b_2) = (a_1a_2 - b_1b_2, a_1b_2 + b_1a_2) = (a_2,b_2)*(a_1,b_1)$. Thus $(A,*)$ is commutative.
We have $(1,0)*(a,b) = (a,b)$ for all $(a,b) \in A$, thus $(1,0) \in A$ is the identity in $(A,*)$.
For all $(a,b) \in A$, as $(a,b) \neq (0,0)$, $a^2 + b^2 \neq 0$, and so we have $\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) \in A$.
Since $(a,b)*\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right) = (1,0)$, it is the inverse of (a,b) in $(A,*)$.

Therefore, $(A,*)$ is an abelian group.

Question 2

Let us be given that $HK = KH$, which is non-empty. 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 $HK \leq G$.

Now instead let us be given that $HK \leq G$.
For any $h \in H$, $k \in K$, we have $(kh)^{-1} = h^{-1}k^{-1} \in HK$. Since HK is a group, 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 3

Since a is a generator of G, we have $b = a^i$ for some $i \in \mathbb{Z}^+$.
For b to be not a generator of G, we have $\gcd(p^n, i) \neq 1$, i.e. $i = p^k$ for some $k \in \mathbb{Z}^+$, $k \leq n$.
This give us $ab = a^{p^k+1}$.

Now since p is a prime and $p \nmid p^k + 1$, we have $\gcd\left(p^k + 1, p^n\right) = 1$.
Thus there exists $s, t \in \mathbb{Z}$ such that $s\left(p^k + 1\right) + tp^n = 1$.
Therefore $a = a^{s\left(p^k+1\right)+tp^n} = \left(a^{p^k+1}\right)^s \left(a^{p^n}\right)^t = (ab)^s \in \langle ab \rangle$, i.e. $G = \langle a \rangle \subseteq \langle ab \rangle$.
Since $\langle ab \rangle \subseteq G$, we conclude that $\langle ab \rangle = G$, i.e. ab is a generator of G.

Question 4

Let $\operatorname{lcm}(a, n) = l$, $\gcd(a, n) = d$, and $\circ(a) = k$. This give us $an = ld$, i.e. $\frac{l}{a} = \frac{n}{d} \in \mathbb{Z}^+$.

Since $\left(\frac{l}{a}\right) a \equiv 0 \mod n$, we have $k \mid \frac{l}{a}$.

Also, we have $ka \equiv 0 \mod n$, i.e. $n \mid ka$. This implies that $\frac{n}{d} \mid k\left(\frac{a}{d}\right)$.
Since $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, by consequence of Euclid's Lemma, we have $\frac{n}{d} \mid k$.

Therefore the order of a is $\frac{l}{a}$.

Question 5

Let $\circ(a) = n \in \mathbb{Z}^+$. We have $a^n = 1_G \in H$, and so $k \leq n$.

Assume on the contrary that $k \nmid n$.
Then by Division Algorithm, there exists $q, r \in \mathbb{Z}_{\geq 0}$ such that $n = kq + r$, where $0 < r < k$.
Since H is a group, $a^r = a^{n-kq} = (a^n)\left(a^k\right)^{-q} = \left(a^k\right)^{-q} \in H$, contradicting the minimality of k.

Therefore $k \mid n$.

Question 6

Since conjugation preserve permutation structure, we have the set of conjugates of σ in S_4 to be,

$$\sigma^{S_4} = \{(\ 1\ \ 2\ )(\ 3\ \ 4\ ), (\ 1\ \ 3\ )(\ 2\ \ 4\ ), (\ 1\ \ 4\ )(\ 2\ \ 3\ )\}.$$

Now τ is a solution iff $\tau\sigma\tau^{-1} = \sigma$, i.e. $\tau \in C_{S_4}(\sigma)$. Notice that $|C_{S_4}| = \dfrac{|S_4|}{|\sigma^{S_4}|} = \dfrac{24}{3} = 8$.

Since $(\ \tau(1)\ \ \tau(2)\ )(\ \tau(3)\ \ \tau(4)\ ) = (\ 1\ \ 2\ )(\ 3\ \ 4\ )$, from the structure, we deduce that $(\ 1\ \ 2\ ), (\ 3\ \ 4\ ), (\ 1\ \ 3\ )(\ 2\ \ 4\ ) \in C_{S_4}$. As $\langle (\ 1\ \ 2\ ), (\ 3\ \ 4\ ), (\ 1\ \ 3\ )(\ 2\ \ 4\ ) \rangle$ is a 8-element subset of C_{S_4}, it is C_{S_4}.

Thus we have,

$$\begin{aligned} C_{S_4} = \ & \{(\ 1\ ), (\ 3\ \ 4\ ), (\ 1\ \ 2\ ), (\ 1\ \ 2\ )(\ 3\ \ 4\ ), (\ 1\ \ 3\ )(\ 2\ \ 4\ ), \\ & (\ 1\ \ 4\ )(\ 2\ \ 3\ ), (\ 1\ \ 4\ \ 2\ \ 3\ ), (\ 1\ \ 3\ \ 2\ \ 4\ )\}. \end{aligned}$$

Question 7

There exists $g \in aH \cap bK$ since it is non-empty.
This give us $g \in aH$ and $g \in bK$, i.e. $gH = aH$ and $gK = bK$.
Thus, $aH \cap bK = gH \cap gK = g(H \cap K)$, i.e. $aH \cap bK$ is a left coset of $H \cap K$ in G.

Question 8

Let $\circ(a_1 a_2 \cdots a_n) = k$, and b_i be the inverse of a_i, $i = 1, 2, \ldots, n$.
Notice that all the b_i's are distinct, thus $G = \{b_1, b_2, \ldots, b_n\}$. Since G is abelian, we have,

$$\begin{aligned}(a_1 a_2 \cdots a_n)^2 &= (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n) \\ &= (a_1 b_1)(a_2 b_2) \cdots (a_n b_n) \\ &= 1_G.\end{aligned}$$

Thus $k \mid 2$.
However the order of G is odd, and so by consequence of Lagrange's Theorem, k is odd.
This implies that $k = 1$, i.e. $a_1 a_2 \cdots a_n = 1_G$.

Question 9

For $g \in G$, $h \in H$, let $ghg^{-1} = a$, i.e. $gh = ag$. This give us $gH = ghH = agH$.
Thus, we have $Hg = Hag$, i.e. $a = (ag)\left(g^{-1}\right) \in H$.

Question 10

There are $\varphi(\varphi(11)) = \varphi(10) = 4$ primitive roots of 11.
Now, $10 = 2 \times 5$. Since,

$$\begin{aligned}2^2 = 4 &\not\equiv 1 \mod 11; \\ 2^5 \equiv -1 &\not\equiv 1 \mod 11,\end{aligned}$$

we conclude that 2 is a primitive root of unity modulo 11.

Now $(\mathbb{Z}/10\mathbb{Z})^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$. Since,

$$\begin{aligned}2^3 &\equiv 8 \mod 11; \\ 2^7 &\equiv 7 \mod 11; \\ 2^9 &\equiv 6 \mod 11,\end{aligned}$$

we have the primitive roots of unity modulo 11 to be $2, 6, 7, 8$.