NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Teo Wei Hao

MA2202 Algebra I
AY 2004/2005 Sem 2

Question 1

Let $a, b, c \in \mathbb{R}\backslash\{0\}$.

$$\begin{aligned}
\text{If } a, b < 0, \quad & (a * b) * c = & ab^{-1}c & = a * (b * c); \\
\text{if } a < 0, b > 0, \quad & (a * b) * c = & ab^{-1}c^{-1} & = a * (b * c); \\
\text{if } a > 0, b < 0, \quad & (a * b) * c = & abc^{-1} & = a * (b * c); \\
\text{if } a, b > 0, \quad & (a * b) * c = & abc & = a * (b * c).
\end{aligned}$$

Thus $(\mathbb{R}\backslash\{0\}, *)$ is associative.
We have $1 * a = a * 1 = a$ for all $a \in \mathbb{R}\backslash\{0\}$, thus $1 \in \mathbb{R}\backslash\{0\}$ is the identity in $(\mathbb{R}\backslash\{0\}, *)$.
For $a \in \mathbb{R}\backslash\{0\}$, we have $a^{-1} \in \mathbb{R}\backslash\{0\}$.
If $a < 0$, then we have $a * a = 1$, and so a is the inverse of a in $(\mathbb{R}\backslash\{0\}, *)$.
If $a > 0$, then we have $a^{-1} * a = a * a^{-1} = 1$, and so a^{-1} is the inverse of a in $(\mathbb{R}\backslash\{0\}, *)$.

Therefore, $(\mathbb{R}\backslash\{0\}, *)$ is a group.

Question 2

Since $H \leq G$, H is non-empty and so K is also non-empty.
Now let $k_1, k_2 \in K$. Then there exists $h_1, h_2 \in H$ such that $k_1 = ah_1a^{-1}$ and $k_2 = ah_2a^{-1}$.
Thus $k_1k_2^{-1} = \left(ah_1a^{-1}\right)\left(ah_2a^{-1}\right)^{-1} = ah_1a^{-1}ah_2^{-1}a^{-1} = a\left(h_1h_2^{-1}\right)a^{-1}$.
Since $h_1h_2^{-1} \in H$, we have $a\left(h_1h_2^{-1}\right)a^{-1} \in K$, and so $K \leq G$.

Question 3

Let $h_1, h_2 \in H$, and $|G| = n$, $n \in \mathbb{Z}^+$, i.e. $n - 1 \in \mathbb{Z}_{\geq 0}$.
Then by consequence of Lagrange's Theorem, we have $h_2(h_2)^{n-1} = h_2^n = 1_G$. Thus $h_2^{-1} = h_2^{n-1}$.
Now since $h_2 \in H$, $h_2^{n-1} \in H$, and since $h_1 \in H$, $h_1h_2^{-1} = h_1h_2^{n-1} \in H$. Thus $H \leq G$.

Question 4

Since $\gcd(m, n) = d$, there exists $s, t \in \mathbb{Z}$ such that $sm + tn = d$.
This give us $a^d = a^{sm+tn} = (a^m)^s + (a^n)^t = (a^m)^s \in \langle a^m \rangle$, i.e. $\langle a^d \rangle \subseteq \langle a^m \rangle$.

Also, there exists $k \in \mathbb{Z}$ such that $kd = m$.
This give us $a^m = a^{kd} = (a^d)^k \in \langle a^d \rangle$, i.e. $\langle a^m \rangle \subseteq \langle a^d \rangle$.

Thus $\langle a^m \rangle = \langle a^d \rangle$.

Question 5

Let $H = A_n \cap G \leq G$ (literally, H is the group of even permutations in G).
Assume that $G - H$ is non-empty, i.e. there exists odd permutations in G. Let $g_1, g_2 \in G - H$.
Since G is a group, $g_2^{-1}g_1 \in G$.
Also $\operatorname{sgn}\left(g_2^{-1}g_1\right) = \operatorname{sgn}(g_2)\operatorname{sgn}(g_1) = (-1)^2 = 1$, and thus $g_2^{-1}g_1 \in A_n$. Therefore $g_2^{-1}g_1 \in H$.
This give us $g_1H = g_2H$ for all $g_1, g_2 \in G - H$.
Thus there are only 2 left cosets of H, namely H and gH for some $g \in G - H$, i.e. $[G : H] = 2$.
Thus $|G - H| = \frac{1}{2}|G|$, i.e. exactly half of the elements of G are odd permutations.

Question 6

Since $H \leq G$, we have $1_G \in H$.
Thus $a = a1_G \in aH \subseteq bK$, i.e. there exists $k_1 \in K$ such that $a = bk_1$. Therefore $a^{-1}b = k_1^{-1}$.
Now for all $h \in H$, there exists $k_2 \in K$ such that $ah = bk_2$. This give us $h = a^{-1}bk_2 = k_1^{-1}k_2 \in K$.
Thus $H \subseteq K$.

Question 7

Let $C_p = \{g \in G \mid g \text{ has order } p\}$. Since G is finite, let there be $t \in \mathbb{Z}^+$ distinct cyclic subgroups of G with order p, namely $H_1, H_2, \ldots, H_t$.
Now let $f : C_p \to \{H_i \mid i \in 1, 2, \ldots, t\}$ such that $f(a) = \langle a \rangle$.
We notice that f is a well-defined function, since for each $a \in C_p$, a is the generator of exactly one cyclic subgroup of order p, which give us $f(a)$ to be defined and unique.

Now since the H_i's are cyclic groups of order p, all its $\varphi(p) = p - 1$ generators are in C_p. This give us $|f^{-1}[H_i]| = p - 1$. Therefore, $|C_p| = \sum_{i=1}^{t} |f^{-1}[H_i]| = t(p - 1)$, and so $(p - 1) \mid C_p$.

Note: We need G to be a finite group.
Else, we can consider $G = (\mathbb{Z}/p\mathbb{Z})[x]$, i.e. the infinite group of all polynomials over $\mathbb{Z}/p\mathbb{Z}$, with normal polynomial addition as the equipped binary operation. Then there are infinitely many elements in G whose order is p (e.g. every elements in the infinite set $\{x^n \mid n \in \mathbb{Z}^+\}$ has order p).

Question 8

Let $h \in H$, $k \in K$.
Since $H \lhd G$, $h^{-1} \in H$ and $k \in G$, there exists $h_1 \in H$ such that $kh^{-1}k^{-1} = h_1$.
This give us $hkh^{-1}k^{-1} = hh_1 \in H$.
Similarly, since $K \lhd G$, $k \in K$ and $h \in G$, there exists $k_1 \in K$ such that $hkh^{-1} = k_1$.
This give us $hkh^{-1}k^{-1} = k_1k^{-1} \in K$.

Thus, $hkh^{-1}k^{-1} \in H \cap K = \{1_G\}$. This implies that

$$\begin{aligned} hkh^{-1}k^{-1} &= 1_G \\ hk &= kh. \end{aligned}$$

Question 9

If n is odd, then $\gcd(2,n)=1$. Thus $\varphi(2n)=\varphi(2)\varphi(n)=\varphi(n)$.

If n is even, then let $n=2^s t$, where $s,t\in\mathbb{Z}^+$ with t being odd.
Using the fact that $\varphi(2^k)=2^{k-1}$ for $k\in\mathbb{Z}^+$, we get

$$\begin{aligned}\varphi(2n) &= \varphi\left(2^{s+1}\right)\varphi(t)\\ &= 2\varphi\left(2^{s}\right)\varphi(t)\\ &= 2\varphi\left(2^{s}t\right)=2\varphi(n).\end{aligned}$$

Question 10

There are $\varphi(\varphi(31))=\varphi(30)=8$ primitive roots of 31.
Now, $30=2\times3\times5$. Since,

$$\begin{aligned}3^6 &\not\equiv 1 \mod 31;\\ 3^{10} &\not\equiv 1 \mod 31;\\ 3^{15} &\not\equiv 1 \mod 31,\end{aligned}$$

we conclude that 3 is a primitive root of unity modulo 31.

Now $(\mathbb{Z}/30\mathbb{Z})^*=\{[1]_{30},[7]_{30},[11]_{30},[13]_{30},[17]_{30},[19]_{30},[23]_{30},[29]_{30}\}$. Since,

$$\begin{aligned}3^7 &\equiv 17 \mod 31;\\ 3^{11} &\equiv 13 \mod 31;\\ 3^{13} &\equiv 24 \mod 31;\\ 3^{17} &\equiv 22 \mod 31;\\ 3^{19} &\equiv 12 \mod 31;\\ 3^{23} &\equiv 11 \mod 31;\\ 3^{29} &\equiv 21 \mod 31,\end{aligned}$$

we have the primitive roots of unity modulo 31 to be $3,11,12,13,17,21,22,24$.