NATIONAL UNIVERSITY OF SINGAPORE
MATHEMATICS SOCIETY

PAST YEAR PAPER SOLUTIONS
with credits to Lin Mingyan Simon

MA2202 Algebra I
AY 2011/2012 Sem 1

Question 1

Denote the permutation given in the question by σ. Then one has $\sigma = (1\,3\,2)(6\,7\,8\,9)\tau$, where we have either $\tau = (4\,5)$ or $\tau = (4)(5)$. Since σ is an even permutation, we must have $\operatorname{sgn}(\sigma) = \operatorname{sgn}((1\,3\,2)(6\,7\,8\,9)\tau) = \operatorname{sgn}((1\,3\,2))\operatorname{sgn}((6\,7\,8\,9))\operatorname{sgn}(\tau) = 1$. As $\operatorname{sgn}((1\,3\,2)) = (-1)^{9-6-1} = 1$ and $\operatorname{sgn}((6\,7\,8\,9)\tau) = (-1)^{9-5-1} = -1$, we must have $\operatorname{sgn}(\tau) = -1$. So τ is an odd permutation, and hence we must have $\tau = (4\,5)$. Therefore, the images of 4 and 5 are 5 and 4 respectively.

Question 2

(a) We observe that for all $a, b, c, d \in \{1, 2, 3, 4\}$ with a, b, c all distinct and b, c, d all distinct, we have $(a\,b\,c)(b\,c\,d) = (a\,b)(c\,d)$. Hence, by making use of this fact, we deduce that $(1\,2)(3\,4) = (1\,2\,3)(2\,3\,4)$.

(b) We note that for all $a, b, c, d, e \in \{1, 2, 3, 4, 5\}$ with a, b, c, d, e all distinct, we have $(a\,b\,c\,d\,e)(a\,b\,e\,d\,c) = (a\,c\,b)$. Hence, by making use of this fact, we deduce that $(1\,2\,3) = (1\,3\,2\,4\,5)(1\,3\,5\,4\,2)$, and $(2\,3\,4) = (2\,4\,3\,1\,5)(2\,4\,5\,1\,3)$. Hence, we have $(1\,2)(3\,4) = (1\,2\,3)(2\,3\,4) = (1\,3\,2\,4\,5)(1\,3\,5\,4\,2)(2\,4\,3\,1\,5)(2\,4\,5\,1\,3)$.

Question 3

We first note that the order of G is equal to the number of integers from 1 to 85 inclusive that is coprime to 86. This gives us $|G| = 86 - \frac{86}{2} - \frac{86}{43} + \frac{86}{86} = 42$. Now, let d be a positive divisor of $|G|$. Since G is cyclic, it follows that there must exist an unique subgroup N of G whose order is equal to d. Therefore, the number of distinct subgroups of G is equal to the number of distinct positive divisors of $|G| = 42 = 2 \cdot 3 \cdot 7$, which is $2 \cdot 2 \cdot 2 = 8$.

Question 4

Let us label the squares of the handkerchief 1-16, from left to right, and top to bottom (so the top left square is labelled 1, and the bottom right square is labelled 16). Let $C = \{c_1, c_2, c_3, c_4\}$ be the set of 4 colours. Let $A = \{(a_1, \cdots, a_{16}) | a_i \in C, i = 1, \cdots 16\}$ denote the set of colourings $(a_1, \cdots, a_{16})$ given to squares 1 to 16 in the ascending order.

Let $g = (1\ 4\ 16\ 13)(2\ 8\ 15\ 9)(3\ 12\ 14\ 5)(6\ 7\ 11\ 10) \in S_{16}$, and denote the group $G = \langle g \rangle$. Note that the order of g is equal to 4 so one has $G = \{e, g, g^2, g^3\}$. We define a group action $\alpha : G \times A \to A$, such that $\alpha(\sigma, (a_1, \cdots, a_{16})) = (a_{\sigma(1)}, \cdots, a_{\sigma(16)})$, where $\sigma \in G$. We note that $A_1, A_2 \in A$ would give rise to the same handkerchief if and only if there exists some $\sigma \in G$ such that $\alpha(\sigma, A_1) = A_2$. Hence, the number of orbits N would correspond to the total number of distinct handkerchiefs.

Now, let $\text{Fix}(\sigma)$ denote the number of elements in A that is fixed by the element σ under the group action α, i.e. $\alpha(\sigma, X) = X$. Note that an element $X \in A$ is fixed by $\sigma \in G$ if and only if the squares of X whose corresponding numbers in the same disjointed cycle of σ have the same colour. Based on this, we see that $\text{Fix}(e) = 4^{16}$, $\text{Fix}(g) = 4^4$, $\text{Fix}(g^2) = 4^8$, $\text{Fix}(g^3) = 4^4$. Hence, by the Burnside's Lemma, we have

$$\begin{aligned} N &= \frac{1}{|G|}\sum_{\sigma\in G}\text{Fix}(\sigma) \\ &= \frac{1}{4}\big(\text{Fix}(e) + \text{Fix}(g) + \text{Fix}(g^2) + \text{Fix}(g^3)\big) \\ &= \frac{1}{4}(4^{16} + 4^4 + 4^8 + 4^4) = 1073758336. \end{aligned}$$

We conclude that there are 1073758336 possible designs of handkerchiefs that can be obtained using 4 different colours.

Question 5

From the first relation, we deduce that $N = 2k + 1$ for some $k \in \mathbb{Z}$. Substituting this into the second relation, we get $2k + 1 \equiv 2 \pmod 3$, or equivalently, $2k \equiv 1 \pmod 3$. This would imply that $k \equiv 4k \equiv 2 \cdot 2k \equiv 2 \cdot 1 \equiv 2 \pmod 3$. Hence, we have $k = 3m + 2$ for some $m \in \mathbb{Z}$, and consequently $N = 2k + 1 = 6m + 5$.

By substituting the last equation into the third relation, one has $6m + 5 \equiv 4 \pmod 5$, or equivalently, $m \equiv 4 \pmod 5$. Hence, we have $m = 5n + 4$ for some $n \in \mathbb{Z}$, and consequently $N = 6m + 5 = 30n + 29$.

Finally, by substituting the last equation into the fourth relation, one has $30n + 29 \equiv 0 \pmod 7$, or equivalently, $2n \equiv 6 \pmod 7$. This would imply that $n \equiv 3 \pmod 7$. Hence, we have $n = 7r+3$ for some $r \in \mathbb{Z}$, and consequently $N = 30n + 29 = 210r + 119$.

As $N > 0$, we see that the least possible value of N is 119. We check that $N = 119$ indeed satisfies the 4 relations given in the question, so the smallest positive integer N that satisfies the given congruences is 119.

Question 6

Note that $|A_5| = \frac{5!}{2} = 60$. Suppose such a subgroup H of A_5 with $|H| = 30$ exists. Then by Lagrange's Theorem, one has $|A_5 : H| = \frac{|A_5|}{|H|} = \frac{60}{30} = 2$. So H has an index of 2 in A_5 and therefore H is a normal subgroup of A_5, which contradicts the fact that A_5 is simple. So the desired holds.

Question 7

(a) We have

$$\begin{aligned} &f^2(\lambda) = f(f(\lambda)) = f(1-\lambda) = 1 - (1-\lambda) = \lambda, \\ &g^2(\lambda) = g(g(\lambda)) = g\left(\frac{1}{1-\lambda}\right) = \left(1 - \frac{1}{1-\lambda}\right)^{-1} = 1 - \frac{1}{\lambda}, \\ &g^3(\lambda) = g^2(g(\lambda)) = g^2\left(\frac{1}{1-\lambda}\right) = 1 - \left(\frac{1}{1-\lambda}\right)^{-1} = \lambda \end{aligned}$$

for all $\lambda \in \mathbb{R} - \{0, 1\}$. So the order of f and g are 2 and 3 respectively.

(b) We have

$$(f \circ g)(\lambda) = f(g(\lambda)) = f\left(\frac{1}{1-\lambda}\right) = 1 - \frac{1}{1-\lambda},$$
$$(g^2 \circ f)(\lambda) = g^2(f(\lambda)) = g^2(1-\lambda) = 1 - \frac{1}{1-\lambda}$$

for all $\lambda \in \mathbb{R} - \{0,1\}$. So $f \circ g = g^2 \circ f$ as desired.

(c) By making use of the fact that G is generated by f, and g, and making use of parts (a) and (b), we deduce that $G = \left\{\mathrm{id}, g, g^2, f, f \circ g, f \circ g^2\right\}$. Therefore, we have $|G| = 6$.

Question 8

(a) We shall prove by induction that $(ab)^{p^n} = a^{p^n} b^{p^n}$ for all $a, b \in G$, $n \in \mathbb{Z}$, $n \geq 0$. The case $n = 0$ is trivial, and suppose that the proposition holds for some $n = k$ with $k \in \mathbb{Z}$, $k \geq 0$. By induction hypothesis, we have $(ab)^{p^k} = a^{p^k} b^{p^k}$. Then one has

$$(ab)^{p^{k+1}} = \left((ab)^{p^k}\right)^p = \left(a^{p^k} b^{p^k}\right)^p = \left(a^{p^k}\right)^p \left(b^{p^k}\right)^p = a^{p^{k+1}} b^{p^{k+1}}.$$

This completes the induction step so we are done.

Now, take any $a, b \in S$. Then one has $a^{p^m} = e = b^{p^n}$ for some $m, n \in \mathbb{Z}$, $m, n \geq 0$. This implies that

$$\left(ab^{-1}\right)^{p^{m+n}} = a^{p^{m+n}} \left(b^{-1}\right)^{p^{m+n}} = \left(a^{p^m}\right)^{p^n} \left(b^{p^n}\right)^{-p^m} = e^{p^n} e^{-p^m} = e,$$

so $ab^{-1} \in S$. Moreover, for all $g \in G$, we see that gag^{-1} is conjugate to a, so the orders of a and gag^{-1} are the same. Since $a^{p^m} = e$, it follows that the order of a is equal to p^k for some $k \in \mathbb{Z}$, $k \geq 0$. Thus, one has $\left(gag^{-1}\right)^{p^k} = e$, so $gag^{-1} \in S$. Therefore, S is a normal subgroup of G.

(b) Since $(xS)^p = x^p S = S$, it follows that $x^p \in S$, so one has $x^{p^{r+1}} = (x^p)^{p^r} = e$ for some $r \in \mathbb{Z}$, $r \geq 0$. This shows that $x \in S$ so we have $xS = S$ as desired.

Question 9

Suppose there exists some $g \in G$ such that $x = gx^{-1}g^{-1}$. We shall prove by induction that $x = g^{2k-1}x^{-1}g^{1-2k}$ for all $k \in \mathbb{Z}^+$. The case $k = 1$ is trivial, and suppose that the proposition holds for some $k = n$ with $n \in \mathbb{Z}^+$. By induction hypothesis, we have $x = g^{2n-1}x^{-1}g^{1-2n}$. This implies that

$$\begin{aligned} x &= g^{2n-1}x^{-1}g^{1-2n} = g^{2n-1}\left(gx^{-1}g^{-1}\right)^{-1}g^{1-2n} = g^{2n-1}gxg^{-1}g^{1-2n} = g^{2n}xg^{-2n}, \\ x &= g^{2n}xg^{-2n} = g^{2n}\left(gx^{-1}g^{-1}\right)g^{-2n} = g^{2(n+1)-1}x^{-1}g^{1-2(n+1)}. \end{aligned}$$

This completes the induction step so we are done.

Now, let the order of g be n. Since $|G|$ is odd and $n \mid |G|$, n must be odd. Therefore, we have $x = g^n x^{-1} g^{-n} = x^{-1}$, and thus $x^2 = e$. Since $x \neq 1_G$, the order of x must be 2. Also, since the order of x must divide $|G|$, we must have $|G|$ to be even, a contradiction. So the desired holds.

Question 10

(a) We have, for all $h_1, h_2 \in H$, and $g \in G$ that $\alpha((e, gH)) = egH = gH$, and $\alpha((h_1h_2, gH)) = (h_1h_2)gH = h_1(h_2gH) = \alpha((h_1, \alpha((h_2, gH))))$. So α is an action of H on G/H.

(b) If H is the trivial subgroup of G or $k = 1$ then the result is trivial. Henceforth we shall assume that $k > 1$, and that $|H| = p^m$, where m is a positive integer and $m < k$.

Firstly, we shall prove that $N(H)$ is a subgroup of G, with $H \subseteq N(H)$. Take $n_1, n_2 \in N(H)$. Then one has $n_1Hn_1^{-1} = H$ and $n_2Hn_2^{-1} = H$. This implies that $n_2^{-1}Hn_2 = H$ so one has $(n_1n_2^{-1})H(n_1n_2^{-1})^{-1} = n_1\left(n_2^{-1}Hn_2\right)n_1^{-1} = n_1Hn_1^{-1} = H$. So $n_1n_2^{-1} \in N(H)$ and hence $N(H)$ is a subgroup of G. Finally, for all $h \in H$, we have $hHh^{-1} = H$ so $h \in N(H)$. We are done.

Next, we shall show that for any $nH \in G/H$, we have $nH \in N(H)/H$, if and only if the orbit of nH under the group action α as defined in part (a) has size 1. If $nH \in N(H)/H$, then one has $n \in N(H)$, so one has $\alpha((h, nH)) = hnH = hHn = Hn = nH$ for all $h \in H$. So the orbit of nH has size 1.

Conversely, take any $nH \in G/H$, and suppose that we have $\alpha((h, nH)) = nH$ for all $h \in H$. Then one has $hnH = nH$ for all $h \in H$. This implies that $n^{-1}hn \in H$ for all $h \in H$, so one has $n^{-1}Hn \subseteq H$. As we have $\left|n^{-1}Hn\right| = |H|$, we must have $n^{-1}Hn = H$, and thus $n^{-1} \in N(H)$. Therefore $n \in N(H)$ so $nH \in N(H)/H$. We are done.

From the above assertion, we deduce that the number of orbits of size 1 must be equal to $|N(H)/H|$, so we have

$$|G/H| = \sum_x |O_x| = |N(H)/H| + \sum_y |O_y|, \tag{1}$$

where the first sum is taken over a representative element x from each orbit, and the second sum is taken over a representative element y from each orbit, where each orbit $|O_y|$ has size strictly larger than 1.

By the Orbit-Stabilizer Theorem, we have $|O_y| = \frac{|H|}{|H_y|}$, where H_y denotes the stabilizer subgroup of y. As H_y is a subgroup of H we have $|H_y|$ to divide $|H| = p^m$. Hence we have $|H_y| = p^n$ for some non-negative integer n. This implies that $|O_y| = p^{m-n} > 1$, so we must have $p||O_y|$. Hence, we must have p to divide the RHS of equation (1).

Also, we note that $|G/H| = \frac{|G|}{|H|} = p^{k-m} > 1$, so $p||G/H|$. So by equation (1) again, we must have $p||N(H)/H|$. Hence, we have $\frac{|N(H)|}{|H|} = |N(H)/H| \geq p > 1$, so $|N(H)| > |H|$. Therefore, we must have $N(H) \neq H$ as desired.